UNIVERSITY OF SOUTHAMPTON

FACULTY OF BUSINESS AND LAW

School of Law

AN ANALYSIS OF THREAT PERCEPTIONS: COMBATING CYBER TERRORISM: THE POLICIES OF NATO AND TURKEY, EVALUATED USING GAME THEORY IN THE CONTEXT OF INTERNATIONAL LAW

By

Mehmet Emin Erendor

Thesis for the Degree of Doctor of Philosophy

January 2017

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF BUSINESS AND LAW

School of Law

Doctor of Philosophy

AN ANALYSIS OF THREAT PERCEPTIONS: COMBATING CYBER TERRORISM: THE POLICIES OF NATO AND TURKEY, EVALUATED USING GAME THEORY IN THE CONTEXT OF INTERNATIONAL LAW

Mehmet Emin Erendor

In 2007 Estonia faced a series of cyber-attacks on its cyber infrastructure, which caused widespread damage to the country's economy, politics and security. However, despite this series of cyber-attacks, NATO did not apply Article 5 of the North Atlantic Treaty due to lack of consensus on applying Article 5 in the Estonian case. Although various approaches have been developed by scholars, there is no common application of international law in the United Nations Charter regarding cyber threats or attacks. Moreover, whilst there has been no common definition of 'cyber terrorism' by the international community, some scholars regard 'cyber-attacks' as acts of war. There is a paucity of literature dealing with the application of international law on cyber threats. A new Strategic Concept was adopted in 2010. Its most important development was to identify the significance of cyber threats to all NATO body members. When updating its own technology, the organisation needs to be ready to defend itself against all kinds of asymmetrical warfare, whether from within or beyond its operational range. At the same time, cyber terrorism and cyber threats have continued to affect all societies within its purview, damaging, threatening, destroying and influencing many states, such as Estonia in 2007, Georgia in 2008, Iran in 2010 and international organisations belonging to NATO in 1999. However, the terms of Article 5 of the North

Atlantic Treaty were imprecise as to whether cyber-attacks can be regarded as a form of threat; for this reason, NATO accepted the case-by-case concept on cyber threats/attacks in terms of the application of Article 5 by the Wales Summit in 2014. Despite the fact that the Charter of the United Nations has not been revised, if its Articles are broadly evaluated, cyber-attacks would be accepted as a threat or use of force against the territorial integrity of a state. The main purpose of this thesis is to analyse and evaluate what has been carried out regarding NATO's operational arrangements and its Cyber Defence approach, and, secondly, to explain this in the lens of Game Theory. Furthermore, it will demonstrate why the web is paramount to NATO's system-driven operations, and why it requires a Cyber Defence arrangement. In particular, the research endeavours to analyse Turkey in this regard. The cyber-attack on Estonia in 2007 will be used by way of a case study to explain the development of threat perceptions, risks, international law, cyber security policies and application of Game Theory.

Keywords: *Cybercrime, Cyber Terrorism, Game Theory, NATO, North Atlantic Treaty, Turkey, Cyber Defence Policy, The United Nations, The UN Charter, NATO Cyber Defence Centre of Excellence, NATO Computer Incident Response Capability (NCIRC)*

TABLE OF CONTENTS

CHAPTER 3: GAME THEORY

CHAPTER 4: THE APPLICATION OF INTERNATIONAL LAW

CHAPTER 5: THE CYBER SECURITY POLICY OF NATO

CHAPTER 6: THE CYBER SECURITY POLICY OF TURKEY

ACADEMIC THESIS: DECLARATION OF AUTHORSHIP

I, Mehmet Emin Erendor declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

AN ANALYSIS OF THREAT PERCEPTIONS: COMBATING CYBER TERRORISM: THE POLICIES OF NATO AND TURKEY, EVALUATED USING GAME THEORY IN THE CONTEXT OF INTERNATIONAL LAW

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;

2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;

3. Where I have consulted the published work of others, this is always clearly attributed;

4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;

5. I have acknowledged all main sources of help;

6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;

7. Either none of this work has been published before submission, or parts of this work have been published as: [please list references below]:

Signed:

Date:

ACKNOWLEDGEMENTS

It was not possible to finish this thesis without the help of certain people around me. If those people had not helped me during my PhD in terms of writing, ideas and motivation, it would have been difficult to finish this programme.

I would firstly like to express my special appreciation and thanks to my supervisor, Mr. Phil Palmer. You have been a tremendous mentor for me and encouraged me to finish my PhD. Your enthusiasm about my project and help with my English has been unforgettable and amazing for me. I have been really happy to work with you on my research project, and I hope we will meet again in the future to talk about more new projects. Your advice on both the research and my career path has been priceless. I would like to thank you again for encouraging my research and for allowing me to grow as a researcher.

A special thanks to my family, particularly to my wife, Tuba Erendor. If she had not understood how difficult the PhD was, and had not encouraged me throughout, it would have been a nightmare for me. Also, I became a father during the course of my PhD. I am grateful to have a taste of this unique experience - when I saw my daughter, Elif’s face during the writing of my thesis, I became even more motivated, to have more time with her. Furthermore, words cannot express how grateful I am to my mother, father, father-in-law, mother-in-law and my brothers for all their support and prayers.

I would also like to thank all of my friends, especially Bünyamin Yıldız, Engin Hasan Çopur and Ahmet Gelgeç who supported me in writing the thesis.

THE LIST OF ABBREVIATIONS

CCDCOE: Cooperative Cyber Defence Centre of Excellence

CDMA: Cyber Defence Management Authority

CDMB: Cyber Defence Management Board

CERT: Computer Emergency Response Team

DDoS: Distributed Denial of Service

DOS: Denial of Service

ICJ: The International Court of Justice

ISI: Institute for Security and Intelligence

ITU: International Telecommunication Unions

NAC: the North Atlantic Council

NATO: North Atlantic Treaty Organisation

NCIRC: NATO Computer Incident Response Capability

NDPP: NATO Defence Planning Process

NGOs: Non-Governmental Organisations

SARF: The Social Amplification of Risk Framework

SCADA: Supervisory Control and Data Acquisition

SOME: Teams for Responding to Cyber Incidents

The EU: The European Union

The UN: The United Nations

TIB: The Telecommunications Communication Presidency

TUBITAK: The Scientific and Technological Research Council of Turkey

TUBITAK UEKAE: The Scientific and Technological Research Council of Turkey National Research Institute of Electronics and Cryptology

ULAKBIM: The Turkish Academic Network and Information Centre

ULAK- CSIRT: Computer Security Incident Response Team

ULAKNET: National Academic Network

UNSC: the United Nations Security Council

USOM: National Cyber Incident Response Centre

USSR: The Union of Soviet Socialist Republics

INTRODUCTION

During the last few decades, cyber-attacks have played a major role in damaging, threatening, destroying and influencing certain targets in the international arena, such as Estonia in 2007, Georgia in 2008 and so on. In particular, the most effective cyber-attack was the series which against Estonia in 2007, which lasted for over three weeks.[1] The purpose behind the cyber terrorist attack was that of blocking the Estonian Government's decision on removing Eastern Block antiquities, particularly the Bronze Soldier. After making this decision, the state faced many cyber-attacks against its governmental and private sectors, the culminating point of these attacks being to block access to the Internet or other information technologies. This case is important in explaining and identifying new cyber policies imposed by states and international organisations, particularly by NATO. One of the main questions of this research is to understand and analyse why the Estonian Case is important for the international community and how it has affected states and regional/international organisations' policies, particularly NATO. Details of these questions will be given separately in Chapter 1, the Estonian Case Study, and Chapter 5, the Cyber Policy of NATO, but the main focus of the research aims to explain NATO's cyber security policy, using the Estonian experience to illustrate the effects of cyber-attacks on states and international or regional organisations. In short, the Estonian case was a significant experience for states and regional/international organisations, because it enabled them to see the effects of cyber terrorist attacks, and correspondingly fix their own vulnerabilities against cyber-attacks. Estonia uses the Internet and information technologies in their daily life as a human right.[2] The significance of the Estonian case was described by Laasme in the following terms:

[1] Czosseck, C., Ottis, R. and Talihärm, A. (eds.) (2011), "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security", *Cooperative Cyber Defence Centre of Excellence*, Tallinn: Estonia, p. 57; Kaska, K., Taliharm, A. and Tikk, E. (eds.) (2011), "Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007", *Cooperative Cyber Defence Centre of Excellence*, Tallinn: Estonia, pp. 41-45

[2] Also Laasme states that: "Between 2005 and 2010, Estonia was considered one of the leading countries in the utilization of digital and electronic infrastructure….. in Estonia, daily life is characterized by hyper-connection, using various mobile technologies and digital innovations, such as e-government and e-Cabinet, e-voting, e-parking, e-banking, e-ID system, e-taxes, e-police, e-prescriptions, electronic health records, digital signing, live-streaming public TV, etc. Briefly, Estonia has attempted to realize anything that it could possibly do by utilizing digital infrastructure, with the aim to make its tiny society more efficient and sustainable under budgetary and demographic constraints. in Estonia, access to the Internet is considered as a basic human right, because it is an essential utility to its citizens for acquiring democratic freedoms." Laasme, H. (2012), "The Role of Estonia in Developing NATO's Cyber Strategy", *Cicero Foundation Great Debate Paper*, No: 12 (8), Available at: http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf (Accessed at: 02/10/2015), pp. 9-10

> "*the increasing dependence on technology to sustain society has made Estonia extremely vulnerable to a myriad of security risks and consequently forced the country to become a driving force of NATO's Cyber Defence Policy*."[3]

Laasme also draws attention to the weakness of NATO and the effect of Estonia on the cyber policy of NATO thus:

> *"Cyber-attacks on Estonia were the impetus for NATO because they forced the Alliance to change its security trajectory into a more comprehensive approach by extending the development of cyber capabilities also to its members. However, taking into account that some of the Allies had already realized their weaknesses in cyber security before the 2002 Prague Summit, the question should not be how Estonia became the driving force of Cyber Policy in NATO, but why it took the Alliance almost thirty years to develop and implement a Cyber Policy and the corresponding strategies*."[4]

It can be understood from these comments that the Estonian case has played a vital role in determining and adopting new cyber security policies, by highlighting the consequences of a cyber-attack, and influencing how states and organisations can identify and determine their policies.

Another important consequence of this attack was the revelation that there is no common international law applicable to and capable of preventing and punishing, cyber terrorism attacks in the international arena. States have been forced to apply international laws to cyber threats, but there are no specific international laws regarding cyber terrorism. For instance, Estonian officials invoked NATO to apply Article 5 of the North Atlantic Treaty, but the organisation applied Article 4 of the Treaty to the Estonian case.[5] For the first time, the application of Articles 4 and 5 of the Treaty was mentioned in the Group of Experts report which was issued by NATO.[6] In the report, experts advised NATO as to how it could

[3] Laasme, H. (2012), "The Role of Estonia in Developing NATO's Cyber Strategy", *Cicero Foundation Great Debate Paper*, No: 12 (8), Available at: http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf (Accessed at: 02/10/2015), pp. 9-10

[4] *Ibid.*, p. 13

[5] Group of Experts Report (2010), "*NATO 2020: Assured Security; Dynamic Engagement*", Available at: http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf (Accessed at: 10/04/2012), p. 45

[6] *Ibid*.

improve its cyber capabilities.[7] Since the experts mentioned that Article 4 should be applied to cybercrimes in the report, NATO evaluated the case of Estonia under that article at the Bucharest Summit in 2008.[8] In NATO Summit in Wales 2014, NATO identified that "*Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis*."[9] With the evaluation of cyber threats under Article 5 of the North Atlantic Treaty, NATO has changed its approach to cyber threats since the Estonian case. Also, the Warsaw Summit in 2016 expanded the scope of cyber threats by including hybrid threats.

One of the main concerns of this research is how the application of international law effectively prevents cyber terrorism. The researcher suggests that international law is not effective in addressing cyber terrorism, because of the inequality of its implementation, and a lack of awareness by international policy-makers about the impact and consequences of cyber terrorism. Besides, it must be mentioned here that the Estonian case was a politically-motivated series of cyber-attacks[10] and that the research will directly focus on the application of the United Nations Charter and North Atlantic Treaty to cyber-attacks in terms of the use of force. As will be detailed in the following chapters, there are many arguments regarding the application of Articles 2/4 and 51 of the UN Charter against cyber-threats, but the UN Security Council have not themselves, applied these Articles for that purpose. Furthermore, scholars argue about how to apply existing international laws against cyber threats, some of them accepting cyber-attacks and cyber threats as acts of war,[11] while others do not.[12] According to Schmitt, cyber threats and attacks can be accepted as acts of war, but such attacks must meet certain requirements, and he suggests that Articles 2/4 and Article 51 of the

[7] Group of Experts Report, *op.cit.*, p. 17

[8] NATO (2008), *Bucharest Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_8443.htm (Accessed at: 02/01/2012); See also; Mcgee, J. (2011), "NATO and Cyber Defense: A Brief Overview and Recent Events' Exercises", *Centre for Strategic and International Studies*, Available at: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events (Accessed at: 03/09/2014)

[9] NATO (2014), *Wales Summit Declaration*, Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (Accessed at: 06/09/2014)

[10] Richards, J. (2009), "Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security", *International Affairs Review*, Vol. XVIII, Available at: http://www.iar-gwu.org/node/65 (Accessed at: 02/10/2015); Tikk, E., Kaska, K., and Vihul, L. (eds.) (2010), *International Cyber Incidents: Legal Considerations*, Estonia: CCD COE Publications, pp. 14-25

[11] Yayla, M. (2013), "Hukuki Bir Terim Olarak Siber Savaş," *TBB Dergisi*, Vol. 104, Available at: http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf (Accessed at: 06/05/2013), p. 188

[12] *Ibid*.

UN Charter should be applied to these kinds of threat.[13] Schmitt's criteria for accepting cyber threats as acts of war can be explained, in brief, as: severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy.[14] Silver criticises Schmitt’s rules, even though he accepts his rule regarding the severity of cyber-attacks. According to Silver, if the attack results in neither death nor damage to property, it is not possible to accept it under international law as an act of war.[15]

The concepts of threat and security are problematic in terms of how they are determined by states and international organisations. Another main aim of this research is to gain a deeper understanding regarding states and international organisations’ perceptions of threat and risk, and the application of international law in relation to such threat perceptions and risks. A brief reference to the historical background that has determined threat perceptions and security policies shows that states and international organisations have changed their security levels in accordance with the dimensions of threats and risks. For instance, the Patriot weapons which were placed in Turkey during 2014 could be regarded as a threat to Iran, but do not have significance for Iraq. Whilst definitions of this concept are examined in greater detail in Chapter 2, it can be said that, even though a situation may have positive consequences for one state, it can be understand by another state as having negative consequences and, ergo, be construed as a threat for that state. When new risks and threats are perceived, states often improve their security capabilities in line with those new risks and threats. In addition, theories also tend to affect the policies of states in terms of the identification and application of policies. Sometimes positivism, sometimes realism and sometimes other theories of international relations and law have had an effect on the policies of states and international organisations. For example, some of NATO’s policies during the Cold War were based on realism.[16] Additionally, international and regional organisations, such as the United Nations and NATO, were established in response to threat perceptions and risks in order to protect peace and security in the international arena.

One of the main problems shared by the international community is terrorism. Even though it is not a recent phenomenon, having occurred in almost every country throughout the world,

[13] Schmitt, M. (1999), “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law*, pp. 914-915

[14] *Ibid*.

[15] Silver, D. B. (2002), “Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter,” *International Law Studies*, Vol. 76, Available at: https://www.usnwc.edu/Research---Gaming/International-Law/New-International-Law-Studies-(Blue-Book)-Series/International-Law-Blue-Book-Articles.aspx?Volume=76 (Accessed at: 16/05/2015), pp. 90-91

[16] Waltz, K. N. (1979), *Theory of International Politics*. New York, McGraw-Hill Publishers; Walt, S. M. (1987), *The Origins of Alliances*, Ithaca, NY: Cornell University Press

with developments in the fields of science and technology, the terrorist organisations of today have access to weapons of mass destruction, including nuclear and biological weapons, poisoned gases and computers. Hence, the destruction that might be caused by terrorism is now of a much larger magnitude.[17]

The concept of terror was first used in France in 1795[18], the term being applied to a policy of intimidation that was used towards its own citizens. According to Golder and Williams, "*the first legal responses to terrorism and attempts to define the word can be traced to the 20th century. One commentator dates 'the first organized international legal attempt to grapple with the problem of defining terrorism' to the International Conferences for the Unification of Penal Law, a series of events convened in various European capitals throughout the 1920s and 1930s. Since then lawyers, academics, national legislatures, regional organisations and international bodies, such as the United Nations, have produced a bewildering array of definitions*."[19] There are many definitions of the concept of terrorism in the international arena, details of which will be given in Chapter 2, but it is crucial to include some definitions here to identify how international organisations and states define it. The international community attempted to define the concept of terrorism in the International Convention for the Suppression of Financing of Terrorism.[20] According to the Convention;

> "*Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act*."[21]

[17] Thomas, J. (2008), *Cybercrime: A Revolution In Terrorism and Criminal Behaviour Creates Change In The Criminal Justice System*, Available at: http://www.associatedcontent.com/article/44605/cybercrime_a_revolution_in_terrorism_html?page=2&cat=37 (Accessed at: 08/06/2013)

[18] Golder, B. and Williams, G. (2004), "What is 'Terrorism'? Problems of Legal Definition", *UNSW Law Journal*, Vo. 27 (2), Available at: http://www.tamilnation.co/terrorism/terrorism_definition.pdf (Accessed at: 28/04/2016), p. 270

[19] *Ibid*.

[20] Walter, C. (2004), "Defining Terrorism in National and International Law", in Walter, C., Vöneky, S., Röben, V. and Schorkopf, F. (eds.) (2004), *Terrorism as a Challenge for National and International Law: Security Versus Liberty?*, Berlin: Springer, p. 34; Young, R. (2006), "Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation", *Boston College International and Comparative Law Review*, Vol. 29 (1), Available at: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1054&context=iclr (Accessed at: 02/05/2016), p.53

[21] "International Convention for the Suppression of Financing of Terrorism", Available at: http://www.un.org/law/cod/finterr.htm (Accessed at: 02/05/2016); *Ibid*.

The United Kingdom Terrorism Act 2000 defines terrorism as:

> *"(1) The use or threat of action where—*
>
> *(a) the action falls within subsection (2),*
>
> *(b) the use or threat is designed to influence the government* **[***or an international governmental organisation] or to intimidate the public or a section of the public, and*
>
> *(c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.*
>
> *(2)The action falls within this subsection if it—*
>
> *(a) involves serious violence against a person,*
>
> *(b) involves serious damage to property,*
>
> *(c) endangers a person's life, other than that of the person committing the action,*
>
> *(d) creates a serious risk to the health or safety of the public or a section of the public, or (e) is designed seriously to interfere with or seriously to disrupt an electronic system."*[22] [23]

[22] "The Terrorism Act 2000", Available at: http://www.legislation.gov.uk/ukpga/2000/11/contents (Accessed at: 18/04/2016)

[23] The United States (U.S.) explains terrorism and international terrorism within the Title 18 of the U.S. Code. According to the U.S. Code;
"(1) the term "international terrorism" means activities that—
(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
(B) appear to be intended—
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidation or coercion; or
(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
(C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum;
(2) the term "national of the United States" has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act;
(3) the term "person" means any individual or entity capable of holding a legal or beneficial interest in property;
(4) the term "act of war" means any act occurring in the course of—
(A) declared war;
(B) armed conflict, whether or not war has been declared, between two or more nations; or
(C) armed conflict between military forces of any origin; and
(5) the term "domestic terrorism" means activities that—
(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
(B) appear to be intended—
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidation or coercion; or

Lastly, many definitions have been offered by scholars. For example, Enders and Sandler define terrorism as:

> *"Terrorism is the premeditated use or threat to use violence by individuals or sub-national groups in order to obtain a political or social objective through the intimidation of a large audience beyond that of the immediate victims."*[24]

As these definitions demonstrate, terrorism mainly consists of violence, or threat of action including killings, bombings, etc., in order to achieve ideological, political, or religious aims. It is clear that there are many different definitions, and this problem stems from the lack any universally accepted definition.

Although there have been many terrorist attacks in the international arena against states or enemies (politicians or general international structures), 9/11 is widely accepted as one of terrorism's milestones since it forced the international community to take quick decisions in order to obstruct terrorism.[25] Akdoğan *et al* explain the importance of the case as "*the first invocation of Article 5 of the North Atlantic Treaty that is known as the Alliance's collective defines clause.*"[26] After the attack, the international community tried to take certain steps against terrorists/terrorism so as to obstruct their attempts before attack (this has been dubbed "pre-emptive self-defence" or "the Bush Doctrine").[27] Indeed, the 9/11 attacks have even been called a kind of cyber-attack against the international arena by some scholars.[28]

With the development of information technology, states and international organisations have faced new risks and threat perceptions; these include cybercrime and cyber terrorism. New

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
(C) occur primarily within the territorial jurisdiction of the United States." "Title 18 of the U.S. Code", Available at: https://www.law.cornell.edu/uscode/text/18/2331 (Accessed at: 18/04/2016)

[24] Enders, W. and Sandler, T. (eds.) (2006), *The Political Economy of Terrorism*, Cambridge: Cambridge University Press, p. 3

[25] Silke, A. (2008), "Research on Terrorism: A Review of the Impact of 9/11 and the Global War on Terrorism", in Chen, H., Reid, E., Sinai, J., Silke, A. and Ganor, B. (eds.) (2008), *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security*, New York: Springer, p. 28; Argomaniz, J. (2010), "The European Union Post 9/11 Counter-Terror Policy Response: An Overview", *Research Institute for European and American Studies*, Research Paper No. 140, Available at: http://www.rieas.gr/images/rieas140.pdf (Accessed at: 05/04/2016)

[26] Akdoğan, H., Sozer, M. A. and Can, A. (2016), "The Role of NATO and Other International Entities in Counter-Terrorism", in Ekici, S., Akdoğan, H. Ragab, E., Ekici, A. and Warnes, R. (eds.) (2016), *Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations*, Amsterdam: IOS Press, p.2

[27] Murphy, S. (2005), "The Doctrine of Pre-emptive Self-Defence", *Villanova Law Review*, Vol. 699, Available at: http://lsgs.georgetown.edu/programs/nlp/preventivewar/Villanova%20Preemption%20Article%20Final.pdf (Accessed at: 05/10/2013)

[28] Muti, A., Tajer, K. and Macfaul, L. (eds.) (2014), "Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions", *Remote Control Project*, Available at: http://remotecontrolproject.org/wp-content/uploads/2014/10/Vertic-Report.pdf (Accessed at: 08/05/2013), pp.7-9

risks and threat perceptions have pushed states and international organisations to pursue new security policies against these threats. However, there is no agreed understanding or definition of these concepts. This has created problems in terms of the identification and assessment of threats between states and international/regional organisations.

Nowadays, since the international community is literally run on technology (i.e. information technologies), terrorists can use technology in order to threaten society's networked information systems.[29] For example, terrorists can use the Internet and information technologies for achieving specific aims, such as political and economic destabilisation, financing their organisation, transmitting child pornography, or promoting their own propaganda and ideologies. Their main aims may be to create fear in society and harm the critical national infrastructures of any state or international organisation. The Internet is the best way for terrorist organisations to spread their propaganda. This is because nowadays many people have access to the Internet, and terrorists are able to reach them by explaining their ideologies in chat groups or on websites. Also, terrorists are able to steal identity and credit card information in order to finance their organisations.

Cybercrime can be accepted as a major threat to the international community. The introduction, expansion and consumption of information technologies have correlated with an increase in cybercriminal activities.[30] Regarding cyberspace, the Internet is used more and more as a medium for well-managed criminal organisations.[31] Indeed, terrorists often achieve their aims by using the Internet and other information systems.[32] In accordance with recent research, cybercrimes differ from terrestrial crimes in four different ways: "*They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.*"[33] To access the Internet, a certain amount of hacking and programming was necessary,[34] which resulted in the true beginnings of cybercrime. Soon afterwards, "unauthorized access," "denial of service" (DoS) attacks, cyber terrorism, cyber stalking, identity theft, and phishing came into existence. As cybercrimes pose complicated

[29] Mishra, R. C. (2004), *Terrorism Implications of Tactics and Technology*, Delhi: Authorspress, p. preface

[30] Parker, D. (1998), *Fighting Computer Crime: For Protecting Information*, USA: John Wiley, p. 10; See also; Schjolberg, S. (2008), *The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva*, Available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Accessed at: 05/06/2015), p.1

[31] Lyman, M. and Potter, G. (1998), *Organized Crime*, New Jersey: Prenhall, p. 25

[32] Weimann, G. (2004), *How Modern Terrorism Uses the Internet*, Available at: http://www.usip.org/sites/default/files/sr116.pdf (Accessed at: 08/05/2015)

[33] Mcconnell International (2000), "Cybercrime...and Punishment*?" Archaic Laws Threaten Global Information*, Available at: http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf (Accessed at: 14/11/2013), pp. 1-2

[34] *Ibid*.

socio-economic, legal and security dilemmas, the international community has sought, during the last few years, to adopt a set of international and regional measures—namely, the creation of a communications network for sharing information about these crimes. On this basis, new forms of cybercrime present new problems to law-makers and international organisations.

It can be said that cyber-terrorism has evolved since the Cold War. After the fall of the USSR, the international system suddenly changed; many states fell, but just as many were born as a result. This tumultuous period of time engendered the spread of terrorism in its various guises. Terrorists have been able to use these technological tools for achieving their aims. By using technological systems, terrorists have been able to find new tactics for attacking any state according to their organisation's aims and ideologies. This new style of terrorism (i.e. cyber-terrorism) is cheaper than traditional terrorism, because it only needs a computer, an internet connection, and a person who knows the vulnerabilities of information systems and knows how to attack them by means of the Internet. Moreover, according to Hawks, terrorists are able to send viruses to critical systems in order to harm them.[35] Therefore, this new kind of terrorism will able to affect all of humanity.

Arquilla and *et al* describe this situation in the following way:

> *"Indeed, terrorism has long been about 'information'—from the fact that trainees for suicide bombings are kept from listening to international media, through the ways that terrorists seek to create disasters that will consume the front pages, to the related debates about countermeasures that would limit freedom of the press, increase public surveillance and intelligence gathering, and heighten security over information and communications systems. Terrorist tactics focus attention on the importance of information and communications for the functioning of democratic institutions; debates about how terrorist threats undermine democratic practices may revolve around freedom of information issues."*[36]

Just like the concept of terrorism in general, there is no common and agreed definition of cyber terrorism. This will be highlighted in the cyber terrorism section, but a definition can be given to explain it here. According to Denning, cyber terrorism is:

[35] Hawks, B. B. (2011), *Cyber Terror: The Borderless Danger*, Available at: http://www.inter-disciplinary.net/wp-content/uploads/2011/05/banuhawksepaper.pdf (Accessed at: 11/04/2012), p. 1

[36] Arquilla, J., Ronfeldt, D. and Zanini, M. (1999), "Networks, Netwar and Information-Age Terrorism", in Khalilzad, Z., White, J. P. and Marshall, A. (eds.) (1999), *Strategic Appraisal: The Changing Role of Information in Warfare*, Santa Monica: RAND, pp. 104-105

> *"Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not."*[37]

With the change of threat perceptions and the situation in the international arena, such as the collapse of the USSR, NATO had to change its organisational structure, since its primary threat had summarily disappeared, and it accepted its new strategic concept in 1991. According to this strategic concept, NATO changed its structure from threat to risk management. According to Articles 7 and 8 of the 1991 strategic concept;

> 7. *The security challenges and risks which NATO faces are different in nature from what they were in the past. The threat of a simultaneous, full-scale attack on all of NATO's European fronts has effectively been removed and thus no longer provides the focus for Allied strategy. Particularly in Central Europe, the risk of a surprise attack has been substantially reduced, and minimum Allied warning time has increased accordingly.*
> 8. *In contrast with the predominant threat of the past, the risks to Allied security that remain are multi-faceted in nature and multi-directional, which makes them hard to predict and assess. NATO must be capable of responding to such risks if stability in Europe and the security of*

[37] Denning, D. E. (2003), *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, H. Comm. on the Armed Services*, Available at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Accessed at: 07/11/2013); See also; Conway, M. (2004), *Cyberterrorism: Media Myth or Clear and Present Danger?*, Available at: http://doras.dcu.ie/505/1/media_myth_2004.pdf (Accessed at: 29/02/2012), pp.3-4

> *Alliance members are to be preserved. These risks can arise in various ways.*[38]

The details of the risks will be given in Chapter 2, but every new strategic concept,[39] such as the strategic concept of the M.C. 14/2 and the Lisbon Summit Declaration,[40] clarify that terrorism presents an actual, serious risk and threat to the safety and security of the Alliance and its associates. NATO will continue independently and jointly to fight this scourge in accordance with international law and the values of the UN Charter. The Alliance especially improves its capability to deter, to protect, to interrupt and to defend against this threat using the most advanced techniques, having additional consultations with its partners, obtaining better information about its threats, and sharing intelligence between its members.[41]

Furthermore, NATO began attempting to fix its cyber infrastructure with the Estonian case which is a milestone for the changing of its cyber policies (e.g. NATO's accepted cybercrime as being a threat in its new Strategic Concept.)[42]

With accepting the new Strategic Concept and policies[43] of 2011,[44] NATO's new principles regarding cyber defence also extended to include prevention, resilience, and non-duplication.[45] In addition, NATO has promised to help its member states if required.[46] Thus, new institutions and teams have been created by NATO in order to protect its systems from cyber-attacks and to help its members quickly.

The Wales Summit in 2014 also played an important role in terms of developing NATO's cyber defence policy. As mentioned above, the Summit agreed that the organisation's cyber defence policy is part of the group's collective defence, which suggests NATO should apply Article 5 of the Treaty on a case-by-case basis.[47] Also, the Warsaw Summit in 2016 expanded

[38] "The Alliance's New Strategic Concept 1991", Available at: http://www.nato.int/cps/en/natohq/official_texts_23847.htm (Accessed at: 05/05/2016)

[39] The details of these strategic concepts are discussed in Chapter 2

[40] NATO (2010), *Lisbon Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease (Accessed at: 04/06/2013)

[41] Prickard, J. and MacDonald, L. (2004), "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks*", Journal of Information Technology Education,* Vol. 3, Available at: http://www.jite.org/documents/Vol3/v3p279-289-150.pdf (Accessed at: 08/04/2012), p. 243-245

[42] NATO (2012), "Tackling New Security Challenges", *Briefing*, Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120116_new-security-challenges-e.pdf (Accessed at: 16/09/2014)

[43] See Chapter 5 for more details

[44] NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (Accessed at: 04/09/2013)

[45] *Ibid*.

[46] *Ibid*.

[47] NATO (2014), *op.cit.*

the coverage of cyber threats in terms of accepting hybrid threats, and NATO agreed to apply Article 5 of Treaty against hybrid threats.[48]

Turkey is one of the NATO member countries, and its cyber policy is still evolving in terms of applying and adopting these new policies. Turkey has not had a long history of improving its cyber defence capabilities. Although Turkey implemented its first cyber security strategy during the mid-2000s, Turkey did not have any specific National Cyber Security Policy or Action Plan upon which for it to improve its cyber capabilities until 2013.[49] Moreover, even though Turkish officials have adopted some laws to prevent cyber threats which are neither directly nor explicitly linked to cyber-attacks. The term cybercrime was first mentioned in the Turkish Penal Code numbered 765 through the amendment law number 3756 in 1991,[50] and some further rules were gradually added to this Penal Code.[51] There were no any additional progress in this regard until 2004, yet law number 5237 in 2004 was ratified which defined new types of cybercrime, such as "*Access to data processing systems,*[52] *Hindrance or destruction of the system, the deletion or alteration of data,*[53] *the improper use of bank or credit cards*[54] *and the Imposition of Security Precautions on Legal Entities."*[55][56] Turkey took

[48] NATO (2016), *Warsaw Summit Communique,* Available at: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed at: 13/10/2016)

[49] The Ministry of Transport, Maritime Affairs and Communications (2013), *National Cyber Security Strategy and Action Plan 2013-2014,* Available at: http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf (Accessed at: 15/08/2013)

[50] 3756 nolu Kanun (1991), "*765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun*", Sayı: 20901, Available at: http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf (Accessed at: 10/11/2013)

[51] *Ibid*.

[52] ARTICLE 243-(1) Any person who unlawfully enters a part or whole of data processing system or remains there is punished with imprisonment up to one year, or imposed punitive fine.
(2) In case the offenses defined in above subsection involve systems which are benefited against charge, the punishment to be imposed is increased up to one half. (3) If such act results with deletion or alteration of data within the content of the system, the person responsible from such failure is sentenced to imprisonment from six months up to two years.

[53] ARTICLE 244-(1) Any person who hinders or destroys operation of a data processing system is punished with imprisonment from one year to five years. (2) Any person who garbles, deletes, changes or prevents access to data, or installs data in the system or sends the available data to other places is punished with imprisonment from six months to three years. (3) The punishment to be imposed is increased by one half in case of commission of these offenses on the data processing systems belonging to a bank or credit institution, or public institutions or corporations. (4) Where the execution of above mentioned acts does not constitute any other offense apart from unjust benefit secured by a person for himself or in favor of third parties, the offender is sentenced to imprisonment from two years to six years, and also imposed punitive fine up to five thousand days.

[54] ARTICLE 245-(1) Any person who acquires or holds bank or credit cards of another person(s) whatever the reason is, or uses these cards without consent of the card holder or the receiver of the card, or secures benefit for himself or third parties by allowing use of the same by others, is punished with imprisonment from three years to six years, and also imposed punitive fine. (2) Any person who secures benefit for himself or third parties by using a counterfeit bank or credit card is punished with imprisonment from four years to seven years if the act executed does not constitute any offense other than forgery.

[55] ARTICLE 246-(1) Security precautions specific to legal entities are imposed in case of commission of the offenses listed in this section within the frame of activities of legal entities.

some steps towards improving its legal system against cyber threats, although cyber terrorism was not mentioned in the aforementioned documents, even though Turkey has a cyber terrorism problem.

Having highlighted some of organisational and state failures in responding to cyber-attacks, I will use Game Theory to analyse the strategies of states and terrorists with using tables. Chlebik explains why Game Theory is ideal for understanding terrorist/cyber terrorist behaviour: "*Because of the interactions between terrorists and counterterrorism agencies, game theory is an ideal tool for understanding terrorist behaviour, and game theory can also be used to dictate policy for future events*."[57]

Then some of these debates will be applied to Turkey to make recommendations and suggestions as to how Turkey improves its cyber security policies and practices.

I. Objectives of the Research

NATO is a military organisation, which was established in 1949, its aim was to protect its members from any attacks/threats that might emerge from the Eastern Block. After the Cold War, the organisation has changed by its strategic concepts and its structure shift from threat to risk. I evaluate these risks and recent threats in order to show how NATO has changed its structure and duties in response to these risks and new threat perceptions, and how it can protect itself and its allies from these kinds of risks and threats.

NATO plays a more important role than the United Nations (the UN), both in Cold War and Post-Cold War terms, because of the voting problem of the permanent members on the Security Council, which resulted in the system being locked by both sides of the Cold War, the USA and the USSR. With the establishment of the United Nations, peace and security were guaranteed by the organisations under the UN Charter. International organisations and regional organisations, such as the United Nations and NATO, have tried to combat threat perceptions in the international arena with their actions and policies to maintain peace and security but due to the ongoing suspicion between the USA and the USSR many decisions of the Security Council of the UN of which both were members and carried a veto.[58] For

[56] *Ibid*; See also; Dülger, M. V. (2005), *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, Available at: http://www.dulger.av.tr/pdf/bilisimsuclariveyctk.pdf (Accessed at: 10/05/2014)

[57] Chlebik, K. (2010), "Terrorism and Game Theory: From the Terrorists' Point of View", *Pepperdine Policy Review*, Vol. 3, Available at: http://publicpolicy.pepperdine.edu/academics/research/policy-review/2010v3/content/terrorism-and-game-theory.pdf (Accessed at: 03/10/2015), pp. 17-18

[58] The details of the Vetoes list can be found at: "Security Council Veto List", Available at: http://research.un.org/en/docs/sc/quick (Accessed at: 26/04/2016)

example, the USA has used its veto power to support Israel in the case of Palestine[59] and the USSR used the right of veto for new membership of the UN, because the USA vetoed the Soviet republics from joining the United Nations, and the USSR tried to maintain East-West equilibrium in the UN during the Cold War.[60] For this reason, the UN, particularly the Security Council, did not have any power to prevent war and other conflicts. This situation has not, in fact, changed since the Cold War, and the problem still continues.[61] Although each member has the right to one vote, if one of the Security Council permanent members uses the right of veto, the resolution or decision cannot be approved.[62] This situation has created obvious problems in terms of the resolution and decision-making of the UN Security Council and its effect in the international arena.[63] NATO has adapted itself to new risks and threat perceptions since the Cold War, and therefore it is important to research on how NATO has adapted itself the new role. On the other hand, the UN does not have any military capability itself, but has worked together with NATO since the Cold War. This can be seen in many

[59] Mahmood, F. (2013), "Power Versus the Sovereign Equality of States: The Veto, the P-5 and United Nations Security Council Reforms", *Perceptions*, Volume XVIII (4), Available at: http://sam.gov.tr/wp-content/uploads/2014/03/Fakiha_Mahmood.pdf (Accessed at: 15/04/2016), p. 131

[60] Security Council Report (2013), *In Hindsight: The Veto*, Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/2013_11_forecast.pdf (Accessed at: 15/04/2016), p. 2; "Hard Evidence: Who Uses Veto in the UN Security Council Most Often- and for What?", Available at: http://theconversation.com/hard-evidence-who-uses-veto-in-the-un-security-council-most-often-and-for-what-29907 (Accessed at: 15/04/2016); Czajka, A. (2011), *The Analysis of the Veto Power in the United Nations Security Council*, Available at: https://www.academia.edu/4028521/The_analysis_of_the_Veto_Power_in_the_United_Nations_Security_Council_Public_International_Law (Accessed at: 15/04/2016), p. 6; Okhovat, S. (2011), The United Nations Security Council: Its Veto Power and Its Reform, *CPACS Working Paper*, No. 15 (1), Available at: https://sydney.edu.au/arts/peace_conflict/docs/working_papers/UNSC_paper.pdf (Accessed at: 15/04/2016)

[61] The vote right according to Article 27 of the UN Charter, "1) each member of the Security Council shall have one vote. 2) Decisions of the Security Council on procedural matters shall be made by an affirmative vote of nine members. 3) Decisions of the Security Council on all other matters shall be made by an affirmative vote of nine members including the concurring votes of the permanent members; provided that, in decisions under Chapter VI, and under paragraph 3 of Article 52, a party to a dispute shall abstain from voting." "The United Nations Charter", Available at: http://www.un.org/en/documents/charter/chapter1.shtml (Accessed at: 10/06/2014)

[62] This situation is highlighted in the Security Council website: "The creators of the United Nations Charter conceived that five countries — China, France, the Union of Soviet Socialist Republics (USSR) [which was succeeded in 1990 by the Russian Federation], the United Kingdom and the United States —, because of their key roles in the establishment of the United Nations, would continue to play important roles in the maintenance of international peace and security. They were granted the special status of Permanent Member States at the Security Council, along with a special voting power known as the "right to veto". It was agreed by the drafters that if any one of the five permanent members cast a negative vote in the 15-member Security Council, the resolution or decision would not be approved. All five permanent members have exercised the right of veto at one time or another. If a permanent member does not fully agree with a proposed resolution but does not wish to cast a veto, it may choose to abstain, thus allowing the resolution to be adopted if it obtains the required number of nine favourable votes." The United Nations Security Council, *Voting System and Records*, Available at: http://www.un.org/en/sc/meetings/voting.shtml (Accessed at: 30/08/2015)

[63] "The Security Council Veto List", Available at: http://research.un.org/en/docs/sc/quick/veto (Accessed at: 30/08/2015)

cases, such as Kosovo and Libya. Therefore it is essential to examine NATO's new role and its security policy on cyber space for a deeper understanding of the importance of NATO.

With the brief information about the recent role of NATO, the main aim of this research is to discuss NATO's cyber defence policy in the context of international law and to explain what steps could be taken by Turkey to combat cyber terrorism, and to highlight NATO's and Turkey's cyber security policies within the framework of Game Theory. Another aim of this research is to discuss Turkey's own policy towards cyber terrorism in terms of NATO's policy. Furthermore, NATO's policy will be demonstrated by means of its impact on both national (its members) and international level in order to offer some salient suggestions for the organisation. Additionally, the case of Estonia will be analysed so as to show the serious threat cyber-attacks posed to the international community, and how cyber terrorists are likely to attack both states and international organisations. The Estonian experience provides the best example to date in understanding threat perceptions clearly, and provides a potential template for developing recommendations to reduce risks.

This topic has been chosen because Turkey, in particular, is one of the most important members of the organisation and has a large part to play in the decision-making of departments and developing of policies. It is imperative to state here the importance of Turkey for NATO. Turkey joined NATO in 1952.[64] Haffdel states that

> "*Turkey's role in NATO is also central to the alliance's strategic interests in developing the missile defence capability, protecting European territories from threats of ballistic missile proliferation.*"[65]

Haffdel's explanation is important because Turkey is neighbours to problematic states such as Syria, Iraq and Iran. Also, NATO sources states that Turkey was a wing country during the Cold War and is second in terms of providing troops to the Alliance.[66]

Aybet also highlights the importance of Turkey as follows:

> *"Once Turkey joined NATO, it became not just an important asset in the defence of the Middle East but also an essential component of the defence of Western Europe. In this sense, Turkey's geostrategic location, its armed forces, and its position as a flank country were indispensable assets in the*

[64] "Why is Turkey in NATO", Available at: http://www.ibtimes.com/why-turkey-nato-704333 (Accessed at: 07/08/2014); "Turkey's Relations with NATO", Available at: http://www.mfa.gov.tr/nato.en.mfa (Accessed at: 07/08/2014)

[65] Hafdell, S. (2012), "Turkey-NATO Relations at the 60th Anniversary", *Policy Update*, No: 2, Available at: http://www.gpotcenter.org/dosyalar/PU2_NATO_Hafdell_MAR2012.pdf (Accessed at: 07/08/2014), p.3

[66] NATO (2015), *Turkey: NATO, EU and its evolving foreign and security policy*, Available at: http://natolibguides.info/Turkey (Accessed at: 15/05/2016)

> *Alliance's attempts to address the military imbalance in Europe in the face of the Soviet threat. After the fall of the Shah in Iran in 1979… Turkey's strategic role in the Middle East grew in prominence. Throughout this period, for NATO Turkey was a 'functional ally'—one that had a crucial geostrategic location and a powerful, large army. Normatively, Turkey was not one of the drivers of the broader Western grand strategy of a liberal world order. We can argue that the functional nature of this relationship continued into the early post–Cold War period when NATO shifted its emphasis from collective defence to collective security. Turkey's regional prominence grew, with Turkey transformed in strategic importance for the West from being a flank country to a frontline country during the first Gulf War in 1991. But it was still not a driver of regional grand strategy. Its newfound strategic importance after 1991 was still perceived within the Alliance as an 'asset,' albeit a different one with perhaps a more significant role to play. Turkey was still the 'functional' ally despite the fact that it was one of the most significant contributors to the Alliance's out-of-area operations throughout the 1990s."*[67]

Continuing, the author says that "*from 2002 onwards, Turkey started to play a more regionally assertive role, as a more confident and positive EU accession process emerged and as internal security challenges were reprioritized within the context of regional shifts of power."*[68] In addition, Hafdell agrees with Aybet about the importance of Turkey for NATO and the Euro-Atlantic area in terms of its geographical position.[69] It goes without saying that Turkey is a pivotal member of NATO, and that it should therefore incorporate that body's security recommendations. Hence it is important to specify Turkey's policies regarding cyber security.

On the other hand, there is very limited information about how international organisations such as NATO combat the risk and threat of cyber terrorism. This problem generally stems from the concept of cyber terrorism itself. Although the international community is aware of this threat, the scope and nature of the threat has not been properly understood yet. Terrorists could be non-state players who are supported trans-nationally (such as Al-Qaeda cells which

[67] Aybet, G. (2012), "Turkey's Security Challenges and NATO", *Carnegie Europe*, Available at: http://carnegieendowment.org/files/Aybet_Brief.pdf (Accessed at: 07/08/2014), p.2

[68] *Ibid*., p.3

[69] Hafdell, *op.cit*., p.1; See also; Gönül, V. (2010), "Turkey-NATO Relations and NATO's New Strategic Concept", *Turkish Policy Quarterly*, Vol. 9 (1), Available at: http://www.turkishpolicy.com/images/stories/2010-01-tpq/15-21.pdf (Accessed at: 07/08/2014)

have regional or international links), or individual independent terrorists who are not affiliated with any organisation. This problem can be illustrated by considering Schmid's definition of terrorism:

> *"[a]n anxiety-inspiring method of repeated violent action, employed by (semi-)clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – direct targets of violence are not main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organisation), (imperilled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought."*[70]

Schmid's definition is broad, and seeks to cover all the repetitive crimes that utilize fear, including state-sponsored terrorism. However, special kinds of responses are needed to tackle cyber terrorism. Clive Walker mentions his ideas on the need to react to cyber terrorism and special responses as:

> *"A special response may typically be justifiable when terrorism is emanating from a group with capacities to organise collectively on a sustained basis, to engage in sophisticated plans and operations, and to operate independently from normal life or to have the capacity to intimidate normal society into tolerating its presence. If those factors are present, one might concede the need to depart from normal laws of criminal detection and process which often assume (and rely upon) the opposites: lone individuals, inadequate, bungling operations, and individuals who cannot help but leave traces of their wrongdoing and who are powerless to stop being picked up by the forces of law and order."*[71]

According to this explanation, it can be said that the special response is also applicable to cyber-terrorism, because the cyber-terrorism can also has the capacity to intimidate society,

[70] Schmid, A. and Jongman, A. (2005), *Political Terrorism: A New Guide to Actors, Authors Concepts, Data Bases, Theories and Literature,* New Jersey: Transaction Publishers, p. 28

[71] Walker, C. (2006), "Cyber-Terrorism: Legal Principle and Law in the United Kingdom", *Penn State Law Review,* Vol. 110 (3), pp. 626-627

and, most importantly, cyber terrorist attacks includes more sophisticated attacks. Also, regarding the special legislation against cyber-terrorism, Walker states:

> *"In effect, it will include not only cyber*-*terrorism as a form of offence or attack… but also the various ways in which the Internet is being used to sustain and further terrorism. This wider ambit is consistent with the uses of terrorism elsewhere those who assist terrorism through finance or the supply of materials become depicted as terrorists and are dealt with accordingly under special legislation"*[72]

In short, special legislation is justified to protect people and the state from this kind of threat by cyber terrorists and their supporters.

This research seeks to provide a greater understanding of the cyber threat and to offer some alternative methods for national, regional and international organisations' security services.

A further aim of my research is to fill the gap in the literature on Turkey. No research has specifically focused on this topic and, therefore, no one has offered any other way for preventing cyber terrorist attacks in Turkey. There have been many cyber-attacks against Turkey's official institutions, such as the Turkish National Police and some government departments, but these attacks have been averted. For example, cyber-attack occurred in Turkey against the Higher Education Council in 2013, when some documents were stolen by hackers and attackers,[73] creating insecurity for officials. Thus, this study attempts to improve cyber defence policies against cyber-attacks in Turkey, and compare its policies to those of NATO for the purpose of observing any possible deficiencies.

The thesis of this thesis is to provide valuable and comprehensive suggestions for Turkey to improve its own law and policy against cyber terrorists, and for international organisations to develop common laws against these kinds of terrorists' activities. In sum, the hope is to improve Turkish defence policy, particularly combating cyber terrorism and to add wider debate seeking the most effective ways of combating this form of terrorism.

II. Methodology

The overall methodology of this research is to analyse NATO and Turkey's cyber defence policies. In order to understand these issues discussed above the research contains some

[72] *Ibid*., p. 634

[73] "YÖK'e Siber Saldırı", Available at: http://www.gazetevatan.com/yok-e-siber-saldiri--503255-gundem/ (Accessed at: 10/05/2014); "YÖK'e Siber Saldırı", Available at: http://beyazgazete.com/video/anahaber/cnn-turk-12/2013/01/11/yok-e-siber-saldiri-364616.html (Accessed at: 10/05/2014); "Hackerler YÖK'e 123456 Şifresiyle Girmiş", Available at: http://www.memurlar.net/haber/327857/ (Accessed at: 10/05/2014)

official sources from NATO and Turkey. Besides, secondary sources of information, such as the Internet, books and journals including NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) publications will be used to understand the organisation's policy against cyber terrorism or attacks.

It is important to understand terrorism and cyber terrorism's activities on the Internet, and to examine the underlying correlations between terrorist groups and cyber-attacks. In addition, as stated above that the case of Estonia will be critically examined to understand the effects of cyber-attacks on states and international and regional organisations. Furthermore, the cyber-attacks on Estonia will be accessed in order to establish if they should be deemed under international law. The intention is to use primary sources, such as official sources from Estonia, in this part of the thesis, and international law will be used as the criteria for judging the legal status of such acts, utilising the NATO Treaty and the UN Charter. Secondary sources, such as CCDCOE material, books and journals will also be used in this section.

To sum up, the thesis uses different materials, and all documents will help to improve the quality and originality of my research. The researcher hopes this research will be used by states and international/regional organisations, as well as cyber experts, to adopt new recommendations and solutions.

III. Structure and Outline of the Thesis

In Chapter 1, the cyber-attack on Estonia in 2007 is discussed. The Estonian experience highlighted the consequences of a cyber-attack, and is significant because of its influence on how other states and organisations identified and determined their cyber policies. After explaining and analysing the case of Estonia, more details will be given about the new policies that were adopted as a response to these cyber-attacks in 2007.

In the last section of this chapter, the Estonian case will be assessed in the context of international law. Some scholars[74] argue that this attack amounted to cyber terrorism being subjected to Articles 2/4 and 51 of the UN Charter and Articles 4 and 5 of the NATO Treaty. These arguments will be examined with detailed information to clarify the case in terms of international law.

Chapter 2 provides a brief historical background to the concept of the word "threat" which has a definitional dilemma. It seeks to highlight some of the problems in defining the concept,

[74] There are many arguments about the application of Articles 2/4 and 51 of the UN Charter against cyber-attacks. Roscini suggests cyber-attacks/force can be evaluated under these articles. Conversely, Schmidt cannot accept cyber-attacks as acts of war and therefore stipulates that these kinds of attacks cannot be examined under these Articles. These debates will be clarified in Chapter 4 in more detail.

and suggests that a common definition should be developed in order to eliminate its vagueness and ambiguity, and to provide a better and more coherent application of international law.

Chapter 2 also provides an evaluation of the concept of threat in order to clarify the notion in the light of several international relational theories. I use these theories to explain and analyse the concept of threat. Additionally, the Cold War term "threat perception/s" will be discussed in relation to Resolutions of NATO, as well as the theories which have affected NATO's decision-making process over time. 'The concept of risk', 'risk management' and 'risk society' will be clarified in this section, and more detail will be given to analyse why NATO changed its structure from threat to risk management. Finally, post 9/11 risks and threats will be discussed with a particular focus on cyber terrorism.

Chapter 3 details the Game Theory and its applications. The theory is normally applied in the Cold War era to analyse the nuclear arms race and Cuban Missile crisis, but I aim to use Game Theory to analyse cyber security policies of NATO and Turkey. Also, the application of Game Theory to risk will be given in this chapter. Lastly, the Estonian case will be evaluated under the Game Theory.

Chapter 4 considers how the international community and international law perceives new threats and responds to them. In addition, more details will be given about the prohibition of the use of force and the exception of the use of force under international law, in order to shed further light on how international law may be developed. The second part of the chapter discusses the application of international law to cyber threats, in particular to cyber terrorism.

Chapter 5 analyses the cyber security policy of NATO. This chapter consists of five different sections. Firstly, the development of NATO's cyber security policy before 2010 is explained. The declarations flowing from the Prague Summit (2002), the Riga Summit (2006), the Bucharest (2008) and Strasbourg/Kehl Summits (2009) will be analysed and assessed according to how they impacted on NATO's revised policy.

The second section evaluates NATO's policy in the post-Lisbon Summit 2010, which played a major role in determining the framework of NATO's newly revised cyber policy. This will be examined by using the Summit declarations and the Group of Experts' report. Furthermore, the Chicago Summit 2012, Wales Summit 2014 and Warsaw Summit 2016 declarations are respectively considered in order to learn more about their decisions and their effects on the newly revised policy.

The third section analyses NATO's new cyber security policy using Game Theory, in order to provide a theoretical background and to explain the policy with mathematical tools.

Section 4 evaluates NATO’s interpretation and application of international law to cyber-attacks, particularly how it applies to Articles 4 and 5 of the NATO Treaty. A brief assessment will be made on how its member states will be affected by these interpretations and applications. Moreover, arguments regarding how international law applies Articles 4 and 5 of the NATO Treaty will be discussed.

The last section is divided into two different parts. In the first part, the researcher critically analyses NATO’s cyber security policy, identifying its positive and negative sides, which are demonstrated via the decisions made by NATO and the declarations issued by the summits. In the second part of this section, some recommendations will be made about how NATO can improve its cyber capabilities. This section illustrates the weaknesses and negative sides of international organisations. My recommendations are not only for NATO, but also for every international organisation, suggesting how they might improve their cyber security policy and protect peace and security across the international arena.

The last chapter, Chapter 6, is about the cyber security policy of Turkey. Turkey is investigated by the researcher because there is a big gap in the existing literature regarding Turkish cyber security. As is stated in the objectives of this research, one of my aims is to provide valuable and comprehensive recommendations for Turkey to improve its cyber capabilities. Therefore, both the negative and positive aspects of Turkey’s cyber security policy will be analysed. This chapter is divided into four different sections. Firstly, background information about the development of Turkey's cyber security policy will be provided. More details will be included, using meetings documents, reports and cyber exercises in order to proffer a better understanding of Turkish cyber security policy.

In the second section of this chapter, statutes on cybercrime in Turkish law will be explained. The law which directly addresses cyber-attacks and terrorism will be discussed in this section. Furthermore, Turkey’s national laws will be analysed in terms of fighting cyber threats in order to identify their weaknesses.

The third section of the chapter evaluates Turkey’s cyber security policy under Game Theory. No research has been produced to evaluate Turkey’s cyber security using Game Theory, so this thesis is important in offering suggestions and recommendations for Turkey’s national researchers and scholars. This section also provides comprehensive information on how to apply Game Theory in further research on Turkey’s international relations and law.

The last section of this chapter assesses the cyber security policy of Turkey, and recommendations are proffered on how Turkey can improve it. My most fervent wish is that my research will help Turkey to improve its cyber security capabilities.

CHAPTER 1: CASE STUDY OF CYBER TERRORISM: ESTONIA

1.1. Introduction

The international community has faced several cyber-attacks in the recent past, e.g. against NASA (i.e. the USA) in 2006, Estonia in 2007, Georgia in 2008, Iran in 2010 and South Korea in 2013,[75] but as stated in the introduction section, the example of Estonia has been chosen, because the Estonian experience acted as a catalyst for improvements in the cyber security systems of both states and international organisations. Also, the intention is to examine the Estonian cyber-attacks and cyber security policy through the lens of Game Theory for the first time.[76]

The purpose of this chapter is to show a real illustration of how cyber terrorist attacks can be dangerous to states and the wider international community. The contention of the researcher is that the attack on Estonia highlighted the real and present threat of cyber-attack, and forced NATO and its influential member states to take notice. Prior to the attack, states and the international community, particularly NATO, did not show much interest in cyber-attacks and cyber terrorism, but the magnitude of the Estonian incident brought overwhelming international attention to the inadequacy of legal frameworks in the cyber domain, especially in the cross-jurisdictional environment, and to the deficiencies of technologies for mapping attribution. Consequently, cyber experts have concluded that even though the Estonian case represented the serious full-scale cyber-attack on a nation state[77], it could not be considered as a state-sponsored attack. The scale and consequence threshold of the cyber-attacks on Estonia did not constitute armed attacks that would have invoked Article 5 of the North Atlantic Treaty.

[75] For more information: "Cyber Timeline", Available at: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm (Accessed at: 22/02/2015); See also; "25 Biggest Cyber Attacks in History", Available at: http://list25.com/25-biggest-cyber-attacks-in-history/ (Accessed at: 22/02/2015)

[76] There is only one work on the application of Prisoners' Dilemma to Estonian case, but it is not related to analyse cyber security policy. The Estonian Case will be examined in the Game Theory chapter.

[77] Richards, J. (2009), *op.cit.*; Ruus, K. (2008), "Cyber War I: Estonia Attacked from Russia", *European Affairs,* Vol. 9, Issue Number 1-2, Available at: http://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia (Accessed at: 10/01/2015); Applegate, S. D. (2009), *Cyber Warfare: Addressing New Threats in the Information Age*, Available at: https://www.academia.edu/1098261/Cyber_Warfare_-_Addressing_New_Threats_in_the_Information_Age (Accessed at: 15/05/2016); Shackelford, S. J. (2009), "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law,* Vol. 27 (1), Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil (Accessed at: 05/05/2015), p. 15; Hansen, L. and Nissenbaum, H. (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly,* Vol. 53, Available at: https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf (Accessed at: 18/05/2016), p. 1156

In the context of this paper, several questions will be discussed to understand the case and its effect to other states and international/regional organisations. For example, a short information was given about why Estonia case so important for the international community in the introduction part, and this can be highlighted in the next section to understand the case completely, and therefore, following questions will be answered in this chapter.

1) Why was the Estonian case so important for the international community?

2) Why was Estonia faced with such a problem?

3) Did Estonia or the international community ever identify any people or states as cyber terrorists? Is it possible to identify cyber criminals and why might identification being difficult?

4) What did NATO do during the cyber-attacks on Estonia? Did NATO support Estonia's fight against those cyber terrorists?

3.2. The Importance of the Estonian Case

"At the beginning of the 21st century, we face a world of extraordinary challenges—and of extraordinary interconnectedness. We are all vulnerable to new security threats, and to old threats that are evolving in complex and unpredictable ways. Either we allow this array of threats, and our responses to them, to divide us, or we come together to take effective action to meet all of them on the basis of a shared commitment to collective security."[78] Kofi Annan mentions new risks and threats to the international community with these words. Today, the international community has faced and experienced many new risks and threat perceptions[79] which are unpredictable and unprecedented. Sometimes, these problems have occurred in small states[80] but affect the whole of society in terms of improving the security policies. For example, Laasme states that "*the significance of small states within multilateral fora is often underestimated and misunderstood because the focus is rather on power than on influence. In fact, small states have demonstrated that they are capable of acting strategically to preserve*

[78] Annan, K. (2004), "Courage to Fulfil Our Responsibilities", *The Economist*, Available at: http://www.economist.com/node/3445764 (Accessed at: 18/05/2016)

[79] For example, terrorism, cybercrime and cyber terrorism. See Chapter 2 for more details.

[80] Thorhallson defines small states as: "the power of a state is often attributed to quantitative criteria, such as population and territorial size, gross domestic product and military capacity. In these terms, small states are held to be politically, economically and strategically vulnerable and as such, incapable of exerting any real influence in World affairs." Thorhallson, B. (2012), "Small States in the UN Security Council: Means of Influence?", *The Hague Journal of Diplomacy*, Vol. 7, Available at: https://rafhladan.is/bitstream/handle/10802/8801/Small-States-UN-Security-Council-by-Thorhallsson.pdf?sequence=1 (Accessed at: 18/05/2016), pp. 135-136; See also; Lee, M. (2006), *How Do Small States Affect the Future Development of the E.U.*, New York: Nova Science Publishers; Hey, J. A. K. (ed.) (2003), *Small States in World Politics: Explaining Foreign Policy Behavior*, London: Lynne Rienner Publishers

security while contributing to the stability and efficiency of international organisations. In addition, smaller nations are more likely to launch initiatives that appear to be small contributions, but, in time, prove to be major developments. Because these nations have a tendency to suffer from inferiority syndromes they are tempted to 'show their mettle' by trying to excel in their initiatives."[81] The Estonian case can be evaluated under this observation, because, as stated in the Introduction, the cyber-attacks on Estonia had a vital role in effecting cyber security policies of states and international organisations, especially NATO.

Joubert describes the significance of the Estonian case as:

> "*However, the attacks were a true wake-up call for NATO, offering a practical demonstration that cyber-attacks could now cripple an entire nation which is heavily dependent on IT networks. Such a prospect is a new threat for NATO member states, as well as for the integrity and efficient working of the information systems which are vital to the Alliance's core tasks of collective defence and crisis management. As a result, the 2010 NATO Strategic Concept stated that the Alliance would* "*develop further [its] ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations".... The Estonian cyber-attacks revealed important malfunctions in NATO's cyber defence arrangements, forcing the Alliance to reconsider its strategy in order to cope with this growing threat.*"[82]

Hughes' ideas support the ideas of Joubert as: "*As with many significant policy transformations, the impetus for NATO's cyber defence policy was born out of a crisis. The famed bronze Red Army statue incident in Tallinn, Estonia, in the spring of 2007 appeared to be the catalyst for NATO's first cyber defence policy.*"[83]

[81] Laasme, *op.cit.*, p. 9

[82] Joubert, V. (2012), "Five Year's After Estonia's Cyber-Attacks: Lessons Learned for NATO?", *Research Paper*, Available at: http://www.ndc.nato.int/news/news.php?icode=394 (Accessed at: 01/05/2016), pp. 1-2

[83] Hughes, R. B. (2008), "NATO and Global Cyber Defence", in Shepherd, R. (2008), *The Bucharest Conference Papers*, London: Chatham House, p. 41

Although NATO began to produce cyber security policies from the Riga Summit 2002, the Estonian case affected these policies and the organisation has tried to implement and apply new security policies.[84] Fidler *et al* state the importance of the Estonian case as:

> *"Even though NATO started to respond to cyber threats earlier, the cyber-attacks on Estonia in 2007 revealed the inadequacy of NATO's activities and sparked a significant scaling up of NATO political commitment and operational capabilities in this area. The Estonian incident helped bring the stakes of cyber threats into sharper perspective for NATO. Cyber threats presented challenges to NATO's image and reputation, its ability to ensure secure communications supporting military operations conducted by the Alliance, its capabilities to function effectively when cyberspace represents a new battlefield or domain of military conflict, and the ability of NATO members to contribute to the Alliance's objectives and missions."*[85]

In short, the Estonian case is important in terms of the determination of the cyber security policies by states and international/regional organisations, because during this case, the international community learned more about the effect of cyber-attacks and their vulnerabilities on cyber space. For example, as is stated above, NATO changed its cyber security policy after the Estonian case and tried to improve its cyber infrastructure with new policies,[86] and therefore, the Estonian case is crucial for the international community in thinking and applying new policies.

The next heading, Estonia's cyber capabilities and why Estonia faced cyber-attacks will be highlighted and evaluated.

3.3. Cyber-Attacks on Estonia

Estonia has a sprawling internet connection and is one of the most developed countries in Europe in terms of its use of information and communication technologies.[87] Together with

[84] The details of these policies details in Chapter 5

[85] Fidler, D. P., Pregent, R. and Vandurme, A. (2013), "NATO, Cyber Defense, and International Law", *St. John's Journal of International Law&Comparative Law,* Vol. 4(1), Available at: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (Accessed at: 17/05/2016), p. 5

[86] More information about NATO's cyber security policy will be given in Chapter 5

[87] Brookes, P. (2008), "The Cyber Challenge", *The Heritage Foundation,* Available at: http://www.heritage.org/research/commentary/2008/03/the-cyber-challenge (Accessed at: 10/11/2014); Boyd, C. (2004), "Estonia opens politics to the web", *BBC,* Available at: http://news.bbc.co.uk/2/hi/technology/3690661.stm (Accessed at: 10/11/2014); NATO Parliamentary Assembly

this developed technology, Estonia became the first country in the world to use technology for the purposes of having legally binding general elections.[88] Moreover, Estonian people mostly use the Internet for all of their business and banking transactions.[89] In short, Estonia has greatly developed its information and communication technology sector, which is used by the vast majority of its citizens. Herzog quoted Howard Schmidt on the technology of Estonia as: "*Estonia has built their future on having a high-tech government and economy, and they've basically been brought to their knees because of these attacks*."[90]

The background to these attacks is worth explaining in brief. The Estonian Government had started negotiations to become a member of NATO after the Prague Summit in 2002, and joined NATO in 2004.[91] It was also accepted as a member of the European Union in May 2004.[92] Estonia had been a member of the Soviet Union before 1990.[93] By joining NATO, Estonia had taken the decision to move away from its Russian influence, and many Soviet symbols and antiquities were removed, apart from 'the Bronze Soldier'- a World War II Soviet memorial. In 2007, the Estonian Government decided to move the Bronze Soldier[94] from a central location in its capital, Tallinn, to the Estonian Defence Forces cemetery.[95]

(2009), *NATO and Cyber Defence*, Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1782 (Accessed at: 03/12/2013)

[88] Czosseck *et al.*, *op.cit.*, p. 1; Associated Press (2005), *Estonia First to Allow Online Voting Nationwide*, Available at: http://www.nbcnews.com/id/9697336/ns/technology_and_science-tech_and_gadgets/t/estonia-first-allow-online-voting-nationwide/#.U2_g0fmSzXs (Accessed at: 10/01/2014); Broache, A. (2005), *Estonia Pulls Off Nationwide Net Voting*, Available at: http://archive.today/20120713045721/http://news.com.com/Estonia+pulls+off+nationwide+Net+voting/2100-1028_3-5898115.html (Accessed at: 10/01/2014); NATO Parliamentary Assembly, *Ibid*.

[89] *Ibid.*

[90] Herzog, S. (2011), "Revisiting the Estonian Cyber-Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Vol. 2(4), Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss (Accessed at: 20/05/2016), p. 52

[91] *Ibid*., p.50

[92] Estonian Embassy in Ankara, *Bir Bakışta Estonya*, Available at: http://www.estemb.org.tr/tur/estonya (Accessed at: 10/04/2014)

[93] Traynor, I. (2007), "Russia accused of unleashing cyberwar to disable Estonia*"*, *The Guardian*, Available at: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (Accessed at: 08/11/2014)

[94] This memorial was erected because of the victory of the Soviet Army against Nazi Germany and for Soviet Soldiers. Associated Press (2007), *Removal of Soviet War Memorial Sparks Deadly Riots in Estonia*, Available at: http://www.foxnews.com/story/2007/04/27/removal-soviet-war-memorial-sparks-deadly-riots-in-estonia/ (Accessed at: 12/04/2014); Malksoo, M. (2007), *The Fallen 'Bronze Soldier' …(A Response to: Is This the Order we wanted?)*, Available at: http://www.icds.ee/index.php?id=73&tx_ttnews%5Btt_news%5D=164&tx_ttnews%5BbackPid%5D=99&cHash=bcff323714 (Accessed at: 12/04/2014)

[95] Lehti, M., Jutila, M., and Jokisipila, M. (2009), "Never Ending Second World War: Public Performances of National Dignity and Drama of the Bronze Soldier", *Journal of Baltic Studies*, Vol. 39(4), Available at: http://blogs.helsinki.fi/majutila/files/2009/07/nesww.pdf (Accessed at: 12/04/2014), p. 1; Ehala, M. (2009), *The Bronze Soldier: Identity Threat and Maintenance in Estonia*, Available at: http://lepo.it.da.ut.ee/~ehalam/pdf/Identity%20threat.pdf (Accessed at: 12/04/2014), p.2

After the decision to remove the Bronze Soldier, Estonia was subjected to a series of cyber-attacks over a time-span of three weeks.[96]

The vulnerabilities of the Estonia's cyber infrastructure and cyberspace became evident in 2007, when the country encountered a series of cyber-attacks over a three week period between April and May, 2007.[97] Richards explains this series of attacks as "*the world's first cyberwar in the form of a three-week wave of distributed denial-of-service attacks that crippled the country's information technology infra-structure*."[98]

Richards also states that these attacks did not result directly from the removal of the Bronze Soldier, but also stemmed from the socio-political background:

> "*Although the Estonian Parliament's decision to remove the Bronze Soldier memorial from Tallinn's main square served as the main precipitating event, other factors contributed to the vulnerability of Estonia's socio-political landscape. The first involved the scores of disaffected, disillusioned ethnic Russians who had been living within Estonia's borders since the end of the World War II. During the 1944-1991 Soviet occupation of Estonia, large groups of ethnic Russians moved into Estonian territory in search of a better life. By the time the Soviet Union collapsed, ethnic minorities comprised approximately 40 percent of the Estonian population. Whereas the newly formed governments of Latvia and Lithuania extended universal citizenship to all people living within their borders, Estonia refused to do so. Instead, the Estonian government insisted that all non-ethnic Estonians be treated as foreigners, thus forcing any ethnic Russian desiring Estonian citizenship to undergo naturalization. Instead of bringing people of all different ethnicities together under the Estonian banner, this policy served as a barrier to*

[96] Kaska, K., Taliharm, A. M., and Tikk, E. (2010), *op.cit. ;* See also; Wilson, C. (2008), "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", *CRS Report for Congress*, p.7; Kaminski, R. T. (2010), "Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions", *Conference on Cyber Conflict Proceedings 2010*, Estonia, p. 81; Cavelty, M. D. (2011), "Cyber-Allies: Strengths and Weaknesses of NATO's Cyber defence Posture", *IP Global Edition*, Vol. 12 (3), Available at: https://www.academia.edu/562910/Cyber-Allies_Strengths_and_weaknesses_of_NATO_s_cyberdefense_posture (Accessed at: 13/12/2014), p. 12; Gervais, M. (2012), "Cyber Attacks and the Laws of War", *Berkeley Journal of International Law*, Vol. 30(2), Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1422&context=bjil (Accessed at: 15/05/2016), p. 539

[97] Czosseck, C., *et al.., op.cit.*, pp. 1-2; Kaska *et al., op.cit.*, pp. 44-47; Nazario, J. (2009), "Politically Motivated Denial of Service Attacks," in Czosseck, C. and Geers, K. (eds.) (2009), *The Virtual Battlefield: Perspectives on Cyber Warfare*, CCDOE Publications, Estonia: IOS Press, p. 3; Tikk *et al., op.cit.*, p. 15

[98] Richards, *op.cit.*

> *further solidify the division between ethnic Estonians and Russians living within Estonian borders. This division, in turn, created an unstable political situation that Russia would find easy to manipulate*."[99]

These points to these cyber-attacks as being politically motivated.[100] Also, Herzog states that "*this type of transnational digital mobilization to exploit the vulnerabilities of nation-states for political purposes exemplifies the emergent threat of cyber terrorism. James Lewis of the Center for Strategic and International Studies (CSIS) offers a clear definition of this phenomenon, noting that cyber terrorism "is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, and government operations) or to coerce or intimidate a government or civilian population*."[101] Denning's definition of cyber terrorism[102] and Herzog's opinion stresses this series of attacks as examples of cyber terrorism, because they included serious attacks against critical infrastructure and generated fears within society, not to mention the fact that they also led to severe economic losses for Estonia.

As Tikk *et al*. explain:

> *"The attacks had two distinctly different phases, each consisting of several waves of elevated intensity. The first phase took place from April 27 to 29 and was assessed to have been emotionally motivated, as the attacks were relatively simple and any coordination mainly occurred on an ad hoc basis. The first phase was followed by the main, co-ordinated attack phase lasting from April 30 to May 18, which was much more sophisticated, and where the use of large botnets and professional coordination was noticed. Notably, clear correlation was observed between politically significant dates and intensification of attacks."*[103]

The first phase of cyber-attacks on Estonian governmental agencies, banks and other institutions tried to force the Government not to make any decision regarding the Bronze Soldier; the suggestion is that the second phase, involving a much larger attack, can be

[99] *Ibid*.

[100] Iasiello, E. (2013), "Cyber Attack: A Dull Tool to Shape Foreign Policy", *5th International Conference on Cyber Conflict*, Available at: https://ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf (Accessed at: 17/05/2016), p. 5; Nazario, *op.cit.*, p.165. Also he gives some examples of the politically motivated cyber-attacks such as: Hainan Spy Plane Incident in 2001, China and CNN, Georgia and Russia, Russian Elections 2007 and so on. The more details can be found in the book.

[101] Herzog, *op.cit.*, p. 52

[102] See Footnote 37

[103] *Ibid*.

explained only within the context of the Estonian Government's subsequent decision to move the statue.

Thomas Viira provides a useful insight into the scope of the attacks:

> *"In Phase I most of the attacks were relatively simple Denial of Service (DoS) attacks against government organisations web servers and Estonian news portals. In Phase II much more sophisticated, massive (use of larger botnets) and coordinated attacks appeared. Most dangerous were Distributed Denial of Service (DDoS) attacks against some of the critical infrastructure components – against data communication network backbone routers and attacks against DNS servers. Some of these DDoS attacks were successful for a very short time period…Cyber-attacks (mostly DDoS) continued also against government organisations web servers. Since May 10, DDoS attacks against two Estonian biggest banks started. For one of them the attack lasted for almost two days and Internet banking services were unavailable for one hour and thirty minutes…. Several attacks were also performed against media company web sites, e.g. DDoS against web servers and comment spam against media portals. There were periods were media companies limited the commenting in media portals and when it was not possible to access web pages from foreign countries.*"[104]

Following the attacks, the Estonian Defence Minister gave a speech to the international media pleading for the European Union and NATO's help. According to him, "*taking into account what has been going on in Estonian cyber-space, both the EU and NATO clearly need to take a much stronger approach and cooperate closely to develop practical ways of combating cyber-attacks*."[105] After this, NATO sent its experts to help Estonia stop these cyber-attacks.[106] Ruus states that "*… Estonia's CERT team, with the help of international experts, designed and implemented a three-pronged strategic response: quickly bolster the country's server capacity ;find ways to electronically distinguish authentic e-mail traffic from zombie*

[104] Viira, T. (2008), "The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva", *Meridian*, Vol.2 (1), Available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Accessed at: 11/11/2014), p.9

[105] "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-Attacks", Available at: http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-ofwarfarecyberattacks/2007/05/16/1178995207414.html (Accessed at: 10/01/2015)

[106] "NATO Sees Recent Cyber Attacks on Estonia as Security Issue", Available at: http://www.dw.de/nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579 (Accessed at: 10/01/2015)

‘attack traffic’ and prevent it from reaching Estonia’s servers; go on the offensive by locating and neutralizing the bots and zombies.”[107]

The Russian Government was blamed for supporting the cyber-attacks against Estonia.[108] Nevertheless, as Kaminski observed, the “*Estonian Foreign Minister, Urmas Paet would publicly accuse Russia of sponsoring the attack, but would later admit that neither Estonia nor NATO had any direct evidence to support such a claim.*”[109] As Biller explains:

> *“Determining whether the attackers were the Russian government or just angry Russian civilians was never completely answered and represents the difficulty of determining attribution even in large-scale attacks. Estonia estimated at least one million computers were used in the attack. However, this many computers can be controlled [with relative] ease by a hacker using a bot-net. Estonia did discover that many of the attacks were routed through Russian government servers, but again, this was inconclusive. The ambiguity of who conducted the Computer Network Attack (CAN) against Estonia is an excellent example of the difficulty attribution creates in classifying a CNA.*”[110]

As Biller states the difficulty of determining attribution can be explained under the changing nature of threat. Brief information was given in the Introduction section that NATO changed its structure from threat to risks with the collapse of the USSR. Details of the new concept of ‘risk’ will be highlighted in the following chapters, showing that the international community can face different risks and threats such as cyber terrorism. For example, Behnke states the role of NATO against new risks and threats as:

> *“In order to maintain security political competence and agency, NATO must first and foremost fight its new enemies; uncertainty and ambiguity. After all, it is only possible to draw up strategies and tactics if the dangers confronting the Alliance can be mastered cognitively and conceptually. In other words, the end of the Cold War produced an enemy perhaps even more formidable than the Soviet Union. Uncertainty and ambiguity are*

[107] Ruus (2008), *op.cit.*

[108] Wilson (2008), *op.cit.*, p.8

[109] Kaminski, *op.cit.*, p. 81

[110] Biller, J. T. (2012), “Cyber-Terrorism: Finding a Common Starting Point”, *Master Thesis,* Available at: http://media.proquest.com/media/pq/classic/doc/2736442311/fmt/ai/rep/NPDF?_s=WeFenx84aXrPIC9W%2FWolUQH7vfo%3D (Accessed at: 15/12/2014), p. 70

> *after all epistemic threats, challenging the very competence and agency of a military-political institution.*"[111]

It may be understood from this that uncertainty and ambiguity are the new enemies of the international community, which should try to improve its security against these.

It should be noted that although the country has a strong background in using cyber infrastructure and the Internet effectively, prior to the attacks, the Estonian Government neglected to implement any effective strategies against cyber-attacks. It should also be noted that it is relatively cheap to conduct a cyber-attack and difficult to locate those responsible, especially when complicated computer network systems are used, which utilise different codes for the purpose of attacking any given state. Although Estonia attributed blame on Russia, because the attackers used Russian websites and servers, no one - not even the special investigative committees convened for determining who was guilty for the attacks were able to find any solid evidence to blame the Russian Government for these attacks.[112] Jaak Aaviksoo, Estonia's Defense Minister said, "…*yesterday that some of the attackers early in the onslaught had been identified as using internet provider addresses from Russian state institutions…[But]There is not sufficient evidence of a [Russian] governmental role.*"[113] Following the attack the Chair of Estonia's Cyber-defence Co-ordination Committee, Mikhel Tammet said:

> *"NATO and the European Union had to establish how to respond to cyber warfare before other members fell victim to a very 21st Century weapon. This is a kind of terrorism, the act of terrorism is not to steal from a state, or even to conquer it. It is, as the word suggests, to sow terror itself. If a highly IT country cannot carry out its everyday activities, like banking, it sows terror among the people."*[114]

He believed that these kinds of threat should be regarded as terrorism, and that international law obligations should be implemented in order to fight against such attackers. In my view, Tammet is right to analyse the cyber-attacks as a kind of terrorism. The main aim of attackers

[111] Behnke, A. (2013), *NATO's Security Discourse After the Cold War: Representing the West*, Oxon: Routledge, p.80

[112] Wilson (2008), *op.cit.*, p.8

[113] Biller, *op.cit.*. ; See also; Traynor, I. (2007), "Web Attackers used a Million Computers, Says Estonia", *The Guardian,* Available at: http://www.theguardian.com/technology/2007/may/18/news.russia (Accessed at: 15/12/2014)

[114] Blomfield, A. (2007), *Estonia Calls for NATO Cyber-Terrorism Strategy,* Available at: http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html (Accessed at: 15/12/2014)

or cyber terrorists was to instil fear which, in turn, affected the whole of Estonian society. It was therefore reasonable for Estonia to look to the international community to clarify their concerns through the interpretation of international law.

1.4. The Cyber Policy of Estonia

Following the cyber-attacks, the Estonian Government created a cyber strategy that included four main points:

> - *A graduated system of security measures in Estonia should be applied;*
> - *The development of Estonia's expertise in and high awareness of information security should be made to the highest standards of excellence;*
> - *The development of an appropriate regulatory and legal framework for supporting the secure and seamless operability of information systems;*
> - *The promotion of international co-operation aimed at strengthening global cyber security.*[115]

Along with accepting a new cyber security strategy, the Estonian Government stipulated the principles of their national cyber security strategy as follows:

> - *Cyber security action plans should be integrated into the routine processes of national security planning;*
> - *Cyber security should be pursued through the co-ordinated efforts of all concerned stakeholders, of public and private sectors as well as of civil society;*
> - *Effective co-operation between the public and private sectors should be advanced for the protection of critical information infrastructure;*
> - *Cyber security should be based on efficient information security, meaning that every information system owner should be aware of his or her responsibilities in the prudent use of information systems and*

[115] Ministry of Defence (2008), *Cyber Security Strategy*, Available at: http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (Accessed at: 12/01/2015), p.3; See also; NATO Parliamentary Assembly (2009), *op.cit.* Czosseck, C, *et al.*, *op.cit.*, p.58

should also take the necessary security measures to manage the identified risks;

- *A general social awareness of threats in cyberspace and the state of readiness to meet them should be fostered; these are important prerequisites, since every member of the information society is responsible for the security of the network-based instruments or systems in his or her possession;*
- *Estonia should co-operate closely with international organisations and other countries to increase cyber security globally;*
- *Proper attention should be paid to the protection of human rights, personal data and identity;*
- *The development and administration of IT solutions for the provision of public services should be brought into compliance with the Estonian IT Architecture and Interoperability Framework, including the information security framework. In addition, consideration should also be given to internal security.*[116]

By adopting this new strategy Estonia sought to develop its cyber security in order to improve its capabilities against any further similar attack. Furthermore the Estonian cyber security strategy aimed to cement all of its policies within a legal foundation. In their cyber security strategy document of 2008, Estonia stipulated its main goal of developing a legal framework was to produce an effective cyber policy that was in harmony with national technical and political policies. This was a significant aspect of the Estonian approach because, as previously suggested, if states fail to do this, or only vouchsafe one side of the security strategy, they will not improve their cyber security, because legislation is necessary to determine the boundaries of attack.

The cyber security strategy adopted by Estonia could improve NATO's approach to cyber security, with new ideas of finding alternative ways to create the best policies to protect itself from any kind of cyber-attacks.

The main ways of improving these legal measures were:

- *The development of legal definitions for cyber security and cybercrime;*

[116] Ministry of Defence, *op. cit.*, pp. 7-8

- *The development and implementation of legislation for ensuring cyber security, including the introduction of compulsory security measures and standards in critical infrastructure companies and the establishment of minimum information security requirements for all information systems;*
- *Improving existing legislation with a view to ensuring the nation's cyber security;*
- *The drafting of new legislation for the purpose of covering new areas or threats;*
- *The launching of initiatives in international law-making.*[117]

When we examine these goals, it is worth noting the call for a definition, which it is already identified, is a significant problem for the international community when it comes to cyber terrorism. It is significant that Estonia sought to address these issues from the very first step of their strategy.

Estonia's Cyber Security Council was established in 2009. The duty of that Council was that of *"[Contributing] to [the] smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy.*" Furthermore, *"The Council is chaired by the Secretary General of the Ministry of Economic Affairs and Communications.*"[118] The cyber security strategy of Estonia was updated in 2010, with the Estonian Government again strongly advocating that they should reduce the vulnerability of the country's critical information and data communication systems against any kind of cyber threat.[119]

A new cyber security strategy was adopted by Estonia in 2014, and covers the period between 2014 and 2017. The Estonian Government highlighted their specific goals for 2017 as, *"[increasing] cybersecurity capabilities and [raising] the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace*."[120] The new cyber security strategy shows significant improvement in the cyber security policies already adopted. The

[117] *Ibid*, pp. 30-31

[118] Republic of Estonia Ministry of Economic Affairs and Communications, *Cyber Security*, Available at: https://www.mkm.ee/en/objectives-activities/information-society/cyber-security (Accessed at: 12/01/2015)

[119] Riigikogu (2010), *National Security Concept of Estonia*, Available at: http://www.kaitseministeerium.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf (Accessed at: 12/01/2015), p. 18

[120] Ministry of Economic Affairs and Communication (2014), *2014-2017 Cyber Security Strategy*, Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf (Accessed on: 12/01/2015), p. 8

Government encouraged both its civilians and the private sector to participate in developing the best cyber security policy, and to cooperate with its national and international partners in order to achieve that aim. In order to:

> *"Ensure the [nation's] ability to provide national defence in cyberspace, the state's civilian and military resources must be able to be integrated into a functioning whole under the direction of civilian authorities as well as being interoperable with the capabilities of [its] international partners. In addition to conventional military environments, national defence planning must increasingly take cyberspace into account."*[121]

The aftermath of the Estonian cyber-attack illustrated international community the serious nature of these threats and signalled the need for improvements their security capabilities with regards to cyberspace. NATO began to produce new policies for protecting itself and its members from any cyber-attack, including the accrediting of the CCDCOE[122] by NATO for finding new and alternative ways to fight cyber threats.

The next section will examine the Estonia case and policy under the Game Theory, but first brief information will be given about what the Game Theory is, and how it can be applied to cyber terrorism.

1.5. The Assessment of the Estonian Case in the Context of International Law

The Estonian attack raised questions about the application of international law. It was not obvious that a cyber-attack could be classified as a criminal or terrorist event and although the cyber-attacks came from Russian websites and its cyber infrastructure, the investigation could not establish any clear evidence that the Russian Government involvement. Nevertheless the Estonian government asked NATO to apply Article 5 of the North Atlantic Treaty, which provides:

> *"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary,*

[121] *Ibid*, p. 6

[122] More details will be given in Chapter 5

> *including the use of armed force, to restore and maintain the security of the North Atlantic area.*
>
> *Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."*[123]

Article 5 has been invoked only once in its history. In this instance its application was always going to be problematic. The Estonian attack could not be regarded as an armed attack; in addition the Convention on Cybercrime in 2004 regarding cyber threats and cyber-attacks provided no clear international agreements in this area. Therefore, the calls of the Estonian government were always going to prove impossible to apply. For the international community this kind of threat was new and there was no clear common practice of applying international law to this type of event. In short, the application of international law against cyber terrorists or states was problematical because, in part, it was difficult to determine who the cyber criminals are in cyberspace. In any event Article 5 of the North Atlantic Treaty and Article 51 of the UN Charter could not be invoked without any clear evidence that Russia was behind the cyber-attacks against Estonia.

It seems obvious during the Estonian case that mutual or international agreements need to be reached in order to compel states to cooperate when trying to define and identify cyber-crime and criminals, thereby reducing the risk of new problems occurring in the international arena. Furthermore the international community must try to find common definitions and laws to implement against cyber criminals.

1.6. Conclusion

As the details of the Estonian case outlined above make clear, cyber threats will be a big problem in the future for states and international organisations. Czosseck *et al*. state that "*the 2007 attacks have shown that cyber-attacks are not limited to single institutions, but can evolve to a level threatening national security*."[124] Also, Goodman mentions that "*the 2007 cyber-attacks on Estonia illustrate how the Internet creates super-empowered actors. Although Estonia insists that others were involved, only one individual has faced criminal charges for the attacks. If an individual using a personal computer can execute an attack on*

[123] NATO (2005), *NATO and the Scourge of Terrorism: What is Article 5?*, Available at: http://www.nato.int/terrorism/five.htm (Accessed at: 14/01/2015)

[124] Czosseck *et al., op.cit.*, p.58

major national or international targets, then individuals become the equals of states in cyberspace. This poses obvious problems as states attempt to develop an effective cyber deterrence strategy. The deterring of states poses enough of a challenge; deterring super-empowered individuals seems almost impossible."[125] In addition, Herzog supports the idea of Goodman in this: "*the attacks on Estonia will likely encourage future groups of transnational imitators, and the events of Spring 2007 have provided states with important information for the further development and improvement of their own cyber-warfare capabilities*.[126]

Nevertheless, the Estonian experience served to alert the international community on the need to guard against this kind of threat in the future. Moreover, international organisations like NATO, as well as nation states, have been actively attempting to fortify their cyber infrastructures against cyber threats and attacks, the Estonian case having showed the vulnerabilities of states and international organisations. Moreover as stated earlier, the Estonian case is influential because others can learn more about how to formulate their cyber security policies from the Estonia experience.

Additionally, the Estonian case opened up debates on the application of international law rules and North Atlantic Treaty towards cyber-attacks. Estonia identified a set of problems that included the ability of international law to address the issues raised. The application of the international law rules on cyber-attacks will be examined in the following chapter, but the Estonian case was important for NATO, because although NATO applied Article 4 of the North Atlantic Treaty in this case, it took important decisions on the application of Article 5 in subsequent Summits.[127]

To sum up, the Estonian case is influential because others can learn more about how to formulate their cyber security policies from the Estonian experience. Estonia has embarked upon the first and most important step of cyber security, which is that of identifying and describing cyber threats. As will be highlighted in the following chapters, some states and international/regional organisations have not identified or defined threats separately, while Estonia has tried to define them separately, believing that it is important to define and identify threats and to take important measures.

[125] Goodman, W. (2010), *Cyber Deterrence: Tougher in Theory than in Practice?,* Available at: http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf (Accessed at: 20/05/2016), p.112

[126] Herzog (2011), *op.cit*., p. 55

[127] The details of the application of Article 5 of North Atlantic Treaty can be found in Chapter 5, but The Wales Summit in 2014 accepted that the cyber-attacks can be evaluated under Article 5 of Treaty.

In the next chapter, the evaluation of threat will be analysed, examined and highlighted, and more detail will be given about the historical evaluation of threat and risk. Importantly, the chapter will also show the changing nature of threat.

CHAPTER 2: THE HISTORICAL BACKGROUND OF THE CONCEPT OF THREAT AND THE ASSESSMENT OF THE RISK

2.1. Introduction

The purpose of this chapter is primarily to ‘set the scene’ by providing a brief background to the concept of threat and risk and some of the difficult definitional issues that have confronted policy makers, national and international organisations and academics. Before explaining the details of the chapter, it is crucial to explain why the concept of threat perceptions has been chosen as a subject for study. It is precisely because they are not well-defined, and there are no common definitions that therefore ‘concept of threat is used for this research. Also, the concept of risk is chosen to analyse the structural shift of NATO after the Cold War.

Throughout the thesis, the terms of the international arena and international system are used. For the most part, the international arena is used in a broad sense[128] to include States, Governments, Regional and International Organisations, Non-Governmental Organisations (NGOs). The research also includes the media, private sectors, universities and research centre,[129] as well as people because people can effect to change their governments and political systems (for example the fall in the Berlin Wall or the Arab Spring).

The international system is complex and contradictory and in contrast to the pre-Cold War,[130] the Post-Cold War age as a complicated mutual relationship.[131] Gratius explains international system as:

> “*The world not being a static place, predictions tend to be off the mark. Nobody predicted – at least not out loud– the fall of the Berlin Wall, Japan’s loss of influence, the terrorist attacks of September 11th 2001, the upsurge in Islamic fundamentalism, ...without wishing to predict the*

[128] The International Arena is used by researcher to explain States, Governments, NGOs and other sectors which have been explained in the definition.

[129] “Evolution of the International Arena”, Available at: http://www.mandint.org/en/evolution (Accessed at: 25/12/2015)

[130] Gratius, S. (2008), “The International Arena and Emerging Powers: Stabilising or Destabilising Forces?”, *FRIDE*, Available at: http://fride.org/descarga/com_emerging_powers_eng_abr08.pdf (Accessed at: 20/12/2015), p. 1

[131] Sim, Y. S. (2007), “International Relations&Complex Systems Theory”, *Proceedings of the 51th Annual Meeting of the ISSS*, Available at: http://journals.isss.org/index.php/proceedings51st/article/viewFile/607/225 (Accessed at: 10/01/2016), p. 1

> *future, and instead taking the current situation as a starting point, the international system is characterised by two general tendencies;*
>
> *- A new international order which is both uni and multi-polar at the same time; The current constellation of global forces and alliances is much less clear than it was in the two previous stages of the post war international system: (1) the ideological confrontation between two superpowers, and (2) the tripartite world dominated by Europe, the USA and Japan. In this third stage, a world order which is multi-polar and uni-polar at the same time is taking shape. It amounts to an a la carte menu which makes room for both old and new powers as well as old and new alliances. The world is uni-polar in the military sphere on account of the clear domination of the USA, and multi-polar in all other international areas.*
>
> *- The (re)enforcing of the nation state and religion; September 11th 2001 saw nation states being strengthened again as the guarantor of national identity and the main protagonists on the world stage, countering the effects of globalisation. At the same time, religion as an instrument of political power is going through a new upsurge. The revitalisation of the intervening state has led to a re-nationalisation of politics and the decline of integration represented above all by the EU."*[132]

As the international system has changed, new actors have emerged in the international arena bringing with them new risks and threats perceptions.

The main purpose of this chapter is to briefly discuss threat perceptions and risks in the international arena from the establishment of the first nation-states or modern states, until recent times. I will describe specific threat perceptions during different periods, starting with the French Revolution, in order to examine particular threat and security approaches. Then, the concept of risk will be detailed, because it is known that NATO changed its structural shift with the end of the Cold War from threat to risk management. Therefore, firstly, the concept of threat will be evaluated and then the concept of risk analysed.

States and communities have used the balance of power against the powerful state or alliances.[133] As a simple example, weak states may seek to form coalitions against a powerful

[132] Gratius, *op.cit*., pp.1-2

[133] Stein, G. J. (2013), "Threat Perception in International Relations", in Huddy, L., Sears, D. O., and Levy, J. (eds.) (2013), *The Oxford Handbook of Political Psychology*, 2nd ed., Oxford: Oxford University Press,

state to balance a power differential in order to neutralise a real or perceived risk or threat.[134] However, this simple way of thinking, which accepted a powerful state as a threat has changed over time. New threat perceptions have emerged in the international arena prompting the development of security studies with scholars considering political, economic, social, psychological and theoretical aspects of the perception.

It has been said that the history of security studies starts after World War I[135] with different theories dominating different periods. McSweeney divides these theories into four different groups, which are: political theory with the idea of common security; political science; political economy; and a fourth period, which divided the history of security studies and includes many new theories such as critical theory, feminist theory and constructivism.[136] The first period, according to McSweeney is the, "*the establishment of international relations as an academic discipline in 1919 until the middle of the 1950s, security was understood more as a multi-disciplinary and multi-dimensional problem, requiring the application of international law, international organisation and political theory to the promotion of democracy, international institutions and disarmament*."[137] It was these notions of idealism and liberalism that lead to The League of Nations being established, but the Second World War pointed to a failure in terms of the application of these theories, partly because the international community was not ready to embrace international organisations, and individual states did not want to give up their national security to any international organisations.

The second period began with the Cold War, which McSweeney termed as the Golden Age of realist theory, where the key characteristic became national security. "*This is the golden age, in the sense that it was then that the subject matter became organized as a sub-discipline separate from the wider concerns of international relations, and began to attract the funds, the journals, the prestige, and the policy relevance, which elevated the authority and influence of security studies beyond any of its sub-disciplinary rivals. The concept of 'national security' characterizes the basic idea of this approach.*"[138] National interests were

Available at: http://www.surrey.ac.uk/politics/research/researchareasofstaff/isppsummeracademy/instructors%20/Stein%20-%20Threat%20Perception%20in%20International%20Relations.pdf (Accessed at: 03/07/2012), p.1; Walt, S. (1985), "Alliance Formation and the Balance of World Power", *International Security*, Vol. 9 (4), Available at: http://www.christoph-rohde.de/waltallianceformationandbop1985.pdf (Accessed at:04/07/2012), p.5

[134] *Ibid*.

[135] Rieker, P. (2000), "Security, Integration and Identity Change", *Norwegian Institute of International Affairs*, Available at: https://www.ciaonet.org/attachments/11318/uploads (Accessed at: 03/01/2016), p.2

[136] McSweeney, B. (1999), *Security, Identity and Interests: A Sociology of International Relations*, Cambridge: Cambridge University Press, pp. 28-30

[137] *Ibid*., p. 31

[138] *Ibid*., p. 29

defined as threats, such as the Union of Soviet Socialist Republics (USSR) as a threat to the USA, and vice versa.

The third period has been referred to as "the decline"[139] because the interest of security studies waned and new interests occurred as Baldwin explained, "*interest in security studies did not revive immediately after the Vietnam War; rather the lessened Cold War tensions associated with détente allowed other issues, such as economic interdependence, Third World poverty, and environmental issues, to increase in salience. And the Arab oil embargo served as a sharp reminder that threats to the American way of life emanated from non-military sources, as well as from military ones*."[140]

The fourth period signalled renewed interest in security studies with, according to Baldwin, "*the old national security studies ... replaced by the new international security studies*."[141] With the new international security studies, critical theory, feminist theory, postmodernism and critical security studies have tried to address the problem of security.[142] This has resulted in threats being categorised and defined differently by different scholars. For example, Mackuen, Erikson and Stimson divide threats into two categories: threats against individuals and threats against communities or states.[143] Threats against states or communities may be political, economic, military, social, or cultural. In parallel with the categorization of threat, the concept of threat is defined by Davis as:

> "*A situation in which one agent or group has either the capability or intention to inflict a negative consequence on another agent or group*".[144]

Krahmann's definition includes situations that affect a whole community:

> "*An event with potentially negative consequences for the survival or welfare of a state, a society, or an individual*."[145]

These definitions suggest that the main point in the definitions is the negative consequence to others and how it can affect a whole society.

[139] Baldwin, D. A. (1995), "Security Studies and the End of the Cold War", *World Politics*, Vol. 48, Available at: http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1995)%20Security%20Studies%20and%20the%20End%20of%20the%20Cold%20War.pdf (Accessed at: 15/08/2012), p. 124

[140] *Ibid.*

[141] *Ibid.*

[142] McSweeney, *op.cit.*, p. 30

[143] Mackuen, M., Erikson R. and Stimson, J. (1992), "Peasants or Bankers? The American Electorate and the U.S. Economy", *American Journal of Political Science*, Vol. 86 (3), 597-611

[144] Davis, J. W. (2000), *Threats and Promises: The Pursuit of International Influence*, Baltimore, MD: Johns Hopkins University Press, p.10

[145] Krahmann, E. (2005), "From State to Non-State Actors: The Emerge Of Security Governance", in Krahmann, E. (ed.) (2005), *New Threats and New Actors in International Security*, New York: Palgrave Macmillan, p.4

The understanding and definition of a threat by a state determines the level of security and security policies adopted. Therefore threat and security have a mutual relationship making it important to define the term “security”. There is no accepted definition of the concept of security[146] but it can be defined as the absence of danger or threat. According to Wolfers, security is, in an objective sense, the absence of threats to national values, and in a subjective sense, the absence of the fear of any attack on values.[147] However, Buzan argues over the definition of security. Buzan thinks “*security studies is not just about any threat, but about that class of threats which human communities define as existential (that is, threatening their definition of what constitutes them as a collectivity), and which are accompanied by calls for emergency responses. Such threats do not have to be military, and therefore security studies broaden the agenda from the military sector into other sectors: political, economic, societal, and environmental.”*[148] Buzan rights in his ideas, because threats cannot only come from the military sector and these threats can be political, economic or environmental. Last decades international community deals with the problem of the climate change, and Buzan stresses the need to expand the coverage of the security studies.

In 2010, a Group of Experts[149] produced a document, *NATO 2020: Assured Security; Dynamic Engagement*, providing advice on the new strategic concept. Cyber threats were mentioned several times, including how threats were directed against communication systems and how this situation could harm society.[150] There were also recommendations about how to respond cyber-related crime. Following publication of this document, a new strategic concept was accepted in Lisbon Summit 2010, called *Active Engagement, Modern Defence*.[151] Both documents, together with NATO’s policies will be discussed in detail in a subsequent chapter. NATO and the UN defined threats, and produced legal frameworks and policies to obstruct threats against peace and security. Moreover, the pre-emptive self-defence doctrine

[146] Sheean, M. (2005), *International Security and Analytical Survey*, London: Lynne Rienner Publishers

[147] Wolfers, A. (1962), *Discord and Collaboration: Essays on International Politics*, Baltimore: Johns Hopkins Press, p.150

[148] Buzan, B. (2000), “Change and Insecurity” Reconsidered”, in Croft, S. And Terriff T. (eds.) (2000), *Critical Reflections on Security and Change*, London: Frank Cass, p. 2

[149] The list of the experts; The Chair is Madeleine K. Albright, Vice-Chair Jeroen van der Veer and the members of the group is Ambassador Giancarlo Aragona (Italy), Ambassador Marie Gervais-Vidricaire (Canada), MP Geoff Hoon (United Kingdom), Ambassador Umit Pamir (Turkiye), Ambassador Fernando Perpina-Robert Peyra (Spain), Ambassador Dr Hans- Friedrich von Ploetz (Germany), Bruno Racine (France), Ambassador Aivis Ronis (Latvia), Profesor Adam Daniel Rotfeld (Poland) and Ambassador Yannis-Alexis Zepos (Greece). NATO (2010), *NATO’s New Strategic Concept: Group of Experts*, Available at: http://www.nato.int/strategic-concept/experts-strategic-concept.html (Accessed at: 20/04/2013)

[150] NATO (2010), *NATO 2020: Assured Security; Dynamic Engagement*, Available at: http://www.nato.int/cps/en/natolive/official_texts_63654.htm#p2 (Accessed at: 24/08/2012)

[151] Heads of State and Government (2010), *Active Engagement, Modern Defence*, Available at: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (Accessed at: 24/08/2012)

announced by George W. Bush, the President of the USA, on 1 June 2002 in response to threat perceptions such as terrorism and the rogue states[152] will also be explained in this section. It is to this perception which I now turn, evaluating definitions and new concepts that seek to clarify it. In order to do so I will first address concepts of threat before and during the Cold War.

2.2. A Theoretical Evaluation of the Concept of Threat up to the Cold War

I will begin with a very simple example provided by Thucydides, [153] who is often acknowledged as the first realist philosopher.[154] Kemos states that "*Thucydides study on the Peloponnesian War, which began in 431 B.C. among Greek city-states, Thucydides observed that the strategic interaction of states followed a discernible and recurrent pattern. According to him, within a given system of states, a certain hierarchy among the states determined the pattern of their relations. Therefore, he claimed that while a change in the hierarchy of weaker states did not ultimately affect a given system, a disturbance in the order of stronger states would decisively upset the stability of the system*."[155] Thucydides states the main reason for the war between Athens and Sparta was that Athens was acquiring more power and its army was better than Sparta's, and so Sparta perceived this situation as a threat.[156] Sparta and other Greek cities had to balance the power of Athens, because Athens was becoming more powerful and this created a threat for other Greek cities. Kemos suggests that "*What made the war inevitable was the growth of Athenian power and the fear which this*

[152] Görener, A. Ş., (2004), "The Doctrine of Pre-Emption and the War in Iraq under International Law", *Perceptions*, Available at: http://sam.gov.tr/wp-content/uploads/2012/02/AylinsekerGorener.pdf (Accessed at: 02/10/2015), pp. 37-38

[153] Thucydides (1919), *History of The Peloponnesian War Books 1-8,* Translated by Charles Forster Smith, Cambridge: Cambridge University Press

[154] Political realism is defined by Moseley as, "a theory of political philosophy that attempts to explain, model, and prescribe political relations. It takes as its assumption that power is (or ought to be) the primary end of political action, whether in the domestic or international arena. In the domestic arena, the theory asserts that politicians do, or should, strive to maximize their power, whilst on the international stage, nation states are seen as the primary agents that maximize, or ought to maximize, their power. The theory is therefore to be examined as either a prescription of what ought to be the case, that is, nations and politicians ought to pursue power or their own interests, or as a description of the ruling state of affairs-that nations and politicians only pursue (and perhaps only can pursue) power or self-interest. Political realism in essence reduces to the political-ethical principle that might is right…Political realism assumes that interests are to be maintained through the exercise of power, and that the world is characterised by competing power bases." Moseley, A. (2015), "Political Realism", *Internet Encyclopedia of Philosophy* , Available at: http://www.iep.utm.edu/polreal/ (Accessed at: 03/01/2016)

[155] Kemos, A. (2015), *The Influence of Thucydides in the Modern World,* Available at: http://www.hri.org/por/thucydides.html (Accessed at: 03/01/2016)

[156]Thucydides, *op.cit.*

caused Sparta," Thucydides wrote in order to illustrate the resulting systematic change; that is, "a change in the hierarchy or control of the international political system."[157]

This simple example illustrates the mutual relationship between threat and security. Security can be defined as protecting national borders from any threat[158], such as attacks from other states. However, this is not true for the joint concepts of security and threat, where psychological and sociological impacts have to be taken into consideration. These two concepts complement each other, with the sociological and psychological aspects of security policies affecting other states' security measures and political direction. According to Machiavelli, the concepts of threat and security demonstrate that almost all states will feel threatened by each other. In other words, if a state wishes to continue to protect and exist, it has to have power against others, and this situation creates a relationship between existence and power where power is more important than morality, and security has priority in state matters regardless of morality. [159] Thomas Hobbes mentions this situation in his book, Leviathan, as: nature made all men equal, but this may sometimes change and one can become stronger than another. Man also resembles a machine that protects itself from any threat. Therefore, every man is set against every other man, much like in war. Accordingly, three principles were said to cause disputes. The first principle is competition,[160] which means to be master of others through violence. The second is diffidence,[161] which is for safety and defence. The last principle is that of the glory[162] of reputation over others and their nations.[163] This suggests that inequality, or being stronger or more powerful than others can represent a threat to other states, nations, or the international community. In response to these threat perceptions, nations seek to find a new way to protect themselves from real and perceived threats, and security approaches have changed and become stronger. On the other hand, power, land reclamation, religion and seeking out new security measures could be interpreted as a threat in these terms.

John Locke's ideas are similar to those of Hobbes, but there are some significant differences. According to Locke, one man can have power over another[164] but not absolute power over

[157] Kemos, *op.cit.*

[158] For example, Turkey nowadays try to protect its borders from the threat of ISIS.

[159] Machiavelli, N. (1952), *The Prince*, Oxford: Oxford University Press

[160] Hobbes, T. (1651), *Leviathan,* London, Available at : http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/hobbes/Leviathan.pdf (Accessed at: 10/05/2012) , pp.76-79

[161] *Ibid.*

[162] *Ibid.*

[163] *Ibid.*

[164] Locke, J. (1690), *Second Treatise of Government,* Edited with an Introduction by Macpherson, C. B. (1980), Indiana: Hackett Publishing Company

others. He explains the nature of man and law in the following way: *"Every man hath a right to punish the offender, and be executioner of the law of nature".*[165] He also explains international relations as a state of nature and according to this principle; states should have same power to punish any state which breaches the natural law in the international community.[166]

However, up to the 18th century the security studies were generally limited to discussions of threat perceptions, because threats were perceived in terms of other states' power or land reclamation, security policy strategy and practice.[167] There was an increased interest in security studies after this period, due to the emergence of new threat perceptions, such as revolutions, reform movements and particularly the phenomenon of the nation-state. The French Revolution was a milestone in new security approaches. The work of philosophers such as Hobbes and Locke influenced the revolution. Notions of liberty, individual security and the social contract meant that the French Revolution was the first major social revolution, of far greater dimensions and of deeper purpose than the American Revolution that had preceded it. Only the Russian Revolution of November 1917, which ushered in modern Communism, would rival in world importance what occurred in France between 1789 and 1799. Underlying this extended dramatic development was the new belief that revolution backed by terror was the most effective means to achieve political and, consequently, social change. Edmund Burke in his pamphlet, Reflections on the Revolution in France, condemned the brutality, the interventionist spirit and the radicalism of the French Revolution and argued:

> *"It is with infinite caution that any man should venture upon pulling down an edifice, which has answered in any tolerable degree for ages the common purposes of society, or on building it up again without having models and patterns of approved utility before his eyes."* [168]

The conclusion Burke drew from these events was that the negative impacts of the French Revolution would be felt not only in France and not only in its immediate aftermath, but would potentially change the world for many more decades or even centuries to come.[169]

It was during the Reign of Terror, 1793-1794, that revolutionary tribunals meted out hasty justice. Opponents of the regime, revolutionaries themselves were executed in their thousands, their deaths added up to a new, horrendous activity of modern Western civilization:

[165] *Ibid.*, p.33

[166] *Ibid.*

[167] For example, one of the most important threat was the Ottoman Empire for the European communities until the 19th century, because the Ottoman Empire enlarged its territory from Anatolia to Vienna.

[168] Burke, E. (1969), *Reflections on the Revolution in France,* Baltimore: Penguin, p.152

[169] *Ibid.*

institutionalized violence, the harsh elimination of political opposition, in other words terrorism. The concerns of other nation states was that revolutionary times required terror, not democratic government, sparking the now familiar arguments about "national security" which were then new, but no less disturbing. In this way security policies were shaped by the policies of other countries, and if one felt any threat from the others, it would take up arms. This explains the security policies found in this century and the arms race that developed.

Before the 19th Century, the international community experienced and created new threat perceptions and security policies that were very different to those that were to come. After the First World War idealism began to emerge as an influential theory. Markwell explains idealism and international communities as follows:

> *"By the 'idealists' we have in mind writers such as Sir Alfred Zimmern, S. H. Bailey, Philip Noel-Baker, and David Mitrany in the United Kingdom, and James T. Shotwell, Pitman Potter, and Parker T. Moon in the United States. ... The distinctive characteristic of these writers was their belief in progress: the belief, in particular, that the system of international relations that had given rise to the First World War was capable of being transformed into a fundamentally more peaceful and just world order; that under the impact of the awakening of democracy, the growth of 'the international mind', the development of the League of Nations, the good works of men of peace or the enlightenment spread by their own teaching, it was in fact being transformed; and that their responsibility as students of international relations was to assist this march of progress to overcome the ignorance, the prejudices, the ill-will, and the sinister interests that stood in its way."*[170]

Following the destruction and insecurity caused by the First World War, the international community experienced the concept of threat in both psychological and sociological terms, so it is not surprising that idealism played a major role in terms of producing new policies against threat perceptions as a concept that should be reflected in international law and considered by international organisations. One of the most important policies that emerged was the Democratic Peace Theory. According to President Woodrow Wilson, the international community could prevent conflict through international organisations which would hold states with similar modes of democratic governance to account, making it more

[170] Markwell, D. (2006), *John Maynard Keynes and International Relations*, Oxford: Oxford University Press, p. 3

difficult to make war on one another.[171] This idea, is not new, it can be traced back to Immanuel Kant, whose notion of 'perpetual peace' is very similar. However Kant queried whether it could work in practice:

> *"The only constitution which derives from the idea of the original compact, and on which all juridical legislation of a people must be based, is the republican. This constitution is established, firstly, by principles of the freedom of the members of a society (as men); secondly, by principles of dependence of all upon a single common legislation (as subjects); and, thirdly, by the law of their equality (as citizens). The republican constitution, therefore, is, with respect to law, the one which is the original basis of every form of civil constitution. The only question now is: Is it also the one which can lead to perpetual peace?"*[172]

His answer is that a republican constitution is only one of a number of necessary conditions for perpetual world peace and that if states have democracy within republican constitutions, then there will be no threat or need for security policies.[173] [174]

The League of Nations was founded based on the idea of controlling and stopping conflicts and promoting peace between states.[175] The League of Nations was a product of World War I in the sense that conflict convinced most persons of the necessity of averting another such cataclysm. But its background lay in the visions of men like Immanuel Kant. Preventing war

[171] Brown, M. E., (ed.) (1996), *Debating the Democratic Peace: An International Security Reader*, Cambridge, MA: The MIT Press; Doyle, M. W. (1997), *Ways of War and Peace: Realism, Liberalism, and Socialism*, New York: W. W. Norton; Elman, M.F. (ed.) (1997), *Paths to Peace: Is Democracy the Answer?* Cambridge, MA: The MIT Press; Doyle, M. W. (1983), "Kant, Liberal Legacies, and Foreign Affairs, Part 1", *Philosophy & Public Affairs*, Vol. 12 (3) (Summer 1983), pp. 213-15, 17; Christopher F. G. and Griesdorf, M. (2001), "Winners or Losers? Democracies in International Crisis, 1918–94," *American Political Science Review 95*, No. 3 (September 2001), pp. 633-34; Russett, B. (2009), "Democracy, War and Expansion through Historical Lenses," *European Journal of International Relations*, Vol.15 (9), pp. 11-12

[172] Kant, I. (1795), *Perpetual Peace: A Philosophical Sketch*, Available at: http://www.constitution.org/kant/perpeace.htm#04 (Accessed at: 23/07/2012)

[173] Skirbekk, G. and Gilje, N. (2001), *A History of Western Thought: From Ancient Greece to the Twentieth Century*, London: Routledge, p.288; Carruthers, S. L. (2001), "International History 1900-1945", in Baylis, J. and Smith, S. (eds.) (2001), *The Globalization of World Politics*, Oxford: Oxford University Press, p.56

[174] "In Toward Perpetual Peace, Kant argues that stable peace can come only when all the nations of the earth are such republics, governed by citizens who see the security of their property obtaining only under the universal rule of law rather than by proprietary rulers who can always see a neighbouring state as a potential addition to their own personal property. But in Kant's view even a worldwide federation of republics cannot guarantee world peace: such a federation provides the necessary conditions for peace, but peace can only be realized and maintained by the free choice of all those politicians governing the republics—the "moral politicians"—to do so." "Toward Perpetual Peace", Available at: http://www2.hawaii.edu/~freeman/courses/phil320/21.%20Perpetual%20Peace.pdf (Accessed at: 05/01/2016)

[175] Skirbekk and Gilje, *op.cit*., and Carruthers, *op.cit*.

through collective security[176] and disarmament were the primary goals of the organisation. This reduced threat perceptions and lowered security policies of states. It is perhaps also worth noting that the Covenant of the League of Nations included new threat perceptions, such as human and drug trafficking, global health, prisoners of war and the protection of minorities.[177] In 1949 the fourth Geneva Convention[178], ensured the application of international law for the victims of war and also included the rights and protections of combatants and non-combatants.[179] More international law was developed by the Hague Conventions, which provided the first formal statements on the law of war and war crimes.[180] [181] However, ultimately the rise of National Socialism in Germany and Italy, which fermented during the Second World War, meant that the League of Nations had failed in its important mission. Eloranta mentions them as: "*the failure of the League of Nations had two important dimensions: 1) The failure to provide adequate security guarantees for its members (like an alliance), thus encouraging more aggressive policies especially by the authoritarian states and leading to an arms race; 2) The failure of this organisation to achieve the disarmament goals it set out in the 1920s and 1930s, such as imposition of military spending constraints. These dimensions, including the aggregate explanations of the weaknesses of the League of Nations, have not been explored adequately by the extensive literature on the interwar economic and political turmoil.*"[182] However, there were some successes from the League of Nations. For example, although the Covenant of the League of Nations did not directly include 'human rights',[183] Article 23 of the Covenant[184] was the closest provision to human rights.[185]

[176] The term was first time used after the Napoleonic Wars in the 19th Century to maintain the status quo between European States and others. This period was between 1815 and the First World War (1914). Also this period was known as *"The Concert of Europe".* For more information: Reichard, M. (2006), *The EU-NATO Relationship: a legal and political perspective,* Aldershot: Ashgate Publishing Limited; Rapoport, A. (1995), *The Origins of Violence: Approaches to the Study of Conflict*, New Jersey: Transaction Publishers; Lowe, J. (1990), *The Concert of Europe: International Relations 1814-70,* London: Hodder Arnold

[177] "The Covenant of the League of Nations", Available at : http://avalon.law.yale.edu/20th_century/leagcov.asp (Accessed at: 29/07/2012)

[178] 'which revised and expanded on the first three'

[179] "Geneva Conventions*",* Available at: http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp (Accessed at: 30/07/2012)

[180] For the details of the Hague Convention visit the page: Available at: http://www.hcch.net/index_en.php (Accessed at:02/08/2012)

[181] It is not necessary to give details of these here because the aim of this chapter is to show that the international community has taken some steps against threat perceptions, by using or developing international law.

[182] Eloranta, J. (2005), "Why Did The League of Nations Fail", *Sixth European Historical Economics Society Conference,* Available at: http://www.ata.boun.edu.tr/ehes/Istanbul%20Conference%20Papers-%20May%202005/WHY_DID_THE_LEAGUE_OF_NATIONS_FAIL.pdf (Accessed at: 20/05/2016), p. 2

[183] Cumper, P. (1999), "Human Rights: History, Development and Classification", in Hegarty, A. and Leonard, S. (eds.) (1999), *A Human Rights : An Agenda for the 21st Century,* London: Cavendish Publishing Limited, p.

According to Cumper, " *Article 23 of the Covenant of the League of Nations, which provided that the populations of the mandated territories should be treated fairly, was one reason why a number of Balkan and Eastern European States signed five special minorities treaties at the end of the First World War. These treaties guaranteed the rights of those who belonged to a racial, religious and linguistic minority and, as the Council of the League of Nations had the power to ensure that States complied with their new obligations, minorities were accorded limited (albeit unprecedented) recognition under international law.*"[186] Also, Isa and de Feyter mention the importance of Article 23 as: "*a direct consequence of this Article was the foundation, within the framework of the League of Nations, of the International Labour Organisation (ILO), which performed a task, and continues to do so, which was unprecedented in the area of workers' rights, equality between men and women at work, the exploitation of child labour, the protection of indigenous peoples…*".[187] It seems clear that the League of Nations had tried to protect minorities and showed men and women to be equal at work. The defence of these rights could be accepted as a success of the League of Nations.

During the period of the League of Nations, as the new threats posed by National Socialism emerged, states began to arm themselves in response. In the comparative area of threat perceptions, this situation could be said to be the same as it had been before the 18th Century.

4; Renteln, A. D. (2013), *International Human Rights: Universalism Versus Relativism*, New Orleans: Quid Pro Books

[184] According to Article 23 of the Covenant;
"Subject to and in accordance with the provisions of international conventions existing or hereafter to be agreed upon, the Members of the League:
(a) will endeavour to secure and maintain fair and humane conditions of labour for men, women, and children, both in their own countries and in all countries to which their commercial and industrial relations extend, and for that purpose will establish and maintain the necessary international organisations;
(b) undertake to secure just treatment of the native inhabitants of territories under their control;
(c) will entrust the League with the general supervision over the execution of agreements with regard to the traffic in women and children, and the traffic in opium and other dangerous drugs;
(d) will entrust the League with the general supervision of the trade in arms and ammunition with the countries in which the control of this traffic is necessary in the common interest;
(e) will make provision to secure and maintain freedom of communications and of transit and equitable treatment for the commerce of all Members of the League. In this connection, the special necessities of the regions devastated during the war of 1914-1918 shall be borne in mind;
(f) will endeavour to take steps in matters of international concern for the prevention and control of disease."
"The Covenant of the League of Nations", *op.cit.*

[185] Smith, R. K. M. (2014), *Textbook on International Human Rights*, Oxford: Oxford University Press, p. 22

[186] Cumper, *op.cit.*, p. 4

[187] Isa, F. G. (2006), "International Protection of Human Rights", in Isa, F. G. and de Feyter, K. (eds.) (2006), *International Protection of Human Rights: Achievements and Challenges*, Available at: https://doc.es.amnesty.org/cgi-bin/ai/BRSCGI/International%20Protection%20of%20Human%20Rights:%20Achievements%20and%20Challenges?CMD=VEROBJ&MLKOB=25926890808 (Accessed at: 21/05/2016), p. 22

2.3. The Cold War Term Threat Perceptions

In this section, Cold War threat perceptions will be evaluated within the context of the strategic concepts of NATO and the UN. I will briefly discuss threat perceptions with reference to both organisations and their understanding of threats to peace and security to the international community. Some examples will be given to recount how these perceptions have changed over time. In addition, some theories and security policies will be outlined.

The failure of the League of Nations and the destruction resulting from the Second World War forced states to seek to find a new way to prevent wars and maintain peace and security. The UN[188] was created to replace the League of Nations. Its aim was to foster cooperation between states through international law, international security, economics, human rights and, most importantly, to maintain peace and security. Article 1 of the Charter provides that the role of the UN is:

> *"To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace."*[189]

The maintenance of peace and security are the most important purposes of the United Nations. However, as will be highlighted later on the Charter does not define the concept of threat well enough, as it does not explain which situations can be accepted as threats that do not require the use of force. There is also no clear description of what constitutes a threat against peace.[190] Evans explains this situation as "*the Framers of the Charter intentionally declined to define the concept in order to give the Security Council broad discretion in making threat*

[188] Report of the High-Level Panel on Threats, Challenges and Change, United Nations (2004), *A More Secure World: Our Shared Responsibility*, Available at: http://www.un.org/secureworld/report.pdf (Accessed at: 28/02/2012)

[189] "The United Nation Charter", Available at: http://www.un.org/en/documents/charter/chapter1.shtml (Accessed at:04/08/2012)

[190] Galvan, M. L. D. L. S. (2011), "Interpretation of Article 39 of the UN Charter (Threat to the Peace) by the Security Council: Is the Security Council a Legislator for the Entire International Community", *Anuario Mexicano de Derecho Internacional*, Vol. XI, Available at: http://www.scielo.org.mx/pdf/amdi/v11/v11a6.pdf (Accessed at: 05/05/2016), p. 148; Kelsen, H. (2000), *The Law of the United Nations: A Critical Analysis of Its Fundamental Problems*, New Jersey: The Lawbook Exchange, p. 727

to peace determinations on a case-by-case basis".[191] Additionally, McDougal and Reisman's idea supports the view of Evans: "*for the better securing of the most fundamental Charter purpose of maintaining "international peace and security, the Framers of the United Nations Charter deliberately conferred upon the Security Council, in the provisions of Chapter VII, a very broad competence both to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and to decide upon what measures should be taken to "maintain or restore international peace and security*".[192] It can be seen why the UN Charter does not define such important concepts. If the concept was defined by the framers of the UN Charter, new threat perceptions and risks could not be evaluated under the concept of the threat to peace. For example, Galvan states that civil wars, violations of human rights and terrorism have been as a threat to peace by the Security Council resolutions since 1990.[193]

Two prominent political systems, of the USA and Soviet Russia, emerged during this time, signalling the Cold War, and creating new threat perceptions and security policies, resulting in the two different sides of political contention and developing their own military alliances. The NATO Treaty was signed in 1949, its aim being to provide security against the Soviet threat and, together with the USA, to protect European states against Soviet Russia and communism[194]. The Warsaw Pact was established in 1955 by Russia and its allies (collectively known as the Eastern Block) to counter NATO and its armament policies.

NATO started to produce its own strategic concepts after its founding in December 1949. The first strategic plan or concept related to the defence of the North Atlantic area against armed attack from the Eastern Bloc.[195] The North Atlantic Military Committee developed another strategic concept in 1950, called the M.C. 14/1. According to this document, the USSR posed the most significant threat to the Alliance, and all defence policies and other self-defence attack plans were to be prepared in anticipation of an attack by the USSR.[196] In this document, the Committee indicated that the USSR and its satellites were perceived as a threat and that

[191] Evans, C. E. (1995), "The Concept of "Threat to Peace" and Humanitarian Concerns: Probing the Limits of Chapter VII of the U.N. Chapter", *Transnational Law & Contemporary Problems*, Vol. 5, Available at: http://heinonline.org/HOL/Page?handle=hein.journals/tlcp5&div=16&start_page=213&collection=journals&set_as_cursor=0&men_tab=srchresults (Accessed at: 05/05/2016), p. 219

[192] McDougal, M. S. and Reisman, W. M. (1968), "Rhodesia and the United Nations: The Lawfulness of International Concern", *The American Journal of International Law*, Vol. 62, Available at: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1663&context=fss_papers (Accessed at: 05/05/2016), p. 6; Also see, Kelsen, *op.cit.*, p. 727

[193] Galvan, *op.cit.*

[194] Peterson, J. W. (2011), *NATO and Terrorism: Organisational Expansion and Mission Transformation*, New York: Continuum, p.2

[195] The Secretary of the NATO (1949), *D.C. 6/1 The Strategic Concept for the Defence of the North Atlantic Area*, Available at: http://www.nato.int/docu/stratdoc/eng/a491201a.pdf (Accessed at: 06/08/2012)

[196] North Atlantic Military Committee (1950), *M. C. 14 Strategic Guidance for North Atlantic Regional Planning*, Available at: http://www.nato.int/docu/stratdoc/eng/a500328c.pdf (Accessed at: 06/08/2012)

this capability against the West was going to increase. This threat assessment included the recognition by NATO of the potential threat of nuclear attack and its consequences.[197] However, on the other side, the USSR and its satellites perceived the West posed a similar threat.

NATO's strategic concepts were therefore based on the theory of realism and its subtitle of the balance of power theory. Realist theory provides that immediate military balance obtains the most effective pressure against another, and that power is important.[198]Waltz[199] argues about the distribution of power within a bipolar system, where there are two great powers, and a multipolar system, where there are more than two great powers. He states that bipolar systems are more peaceful than multipolar systems because bipolar systems typically have less military conflicts between states.[200] [201]

Waltz points to the advantages, for security, that bipolar systems have over the multipolar system. These are identified by Rousseau as:

> *"First, the greater number of states in a multipolar system increase uncertainty and the possibility for miscalculation. Second, multipolar systems are prone to "buck-passing". The possibility of buck-passing encourages risk-seeking leaders to underestimate the costs of war, and the occurrence of buck-passing decreases the probability of quickly containing revisionist states. Third, multipolar systems are more dangerous because they are prone to "chain-ganging". Tight alliances leave all members subject to the whims of the most radical member and can facilitate the rapid spread of war after onset. In sum, chain-ganging*

[197] North Atlantic Defense Committee (1950), *D.C. 13 North Atlantic Treaty Organisation Medium Plan*, Available at: http://www.nato.int/docu/stratdoc/eng/a500328d.pdf (Accessed at: 06/08/2012)

[198] Rousseau, D. L. and Retamero, R. G. (2007), "Identity, Power and Threat Perception: A Cross National Experiment Study", *Journal of Conflict Resolution*, Vol. 51 (5), October, Available at: http://www.albany.edu/~dr967231/articles/RousseauJCROct2007.pdf (Accessed at: 10/08/2012), p.746

[199] He is one of the founders of Neorealism.

[200] Rousseau, D. L. (2006), I*dentifying Threats and Threatening Identities: The Social Construction of Realism and Liberalism*, Stanford: Stanford University Press, p.22

[201] There have, of course, been some conflicts, such as the Korean War in 1950, the Vietnam War in 1959 and the Soviet war in Afghanistan in 1979. There have also been many crises in the area which can be regarded as a threat. One of them was experienced in 1962 between the USSR and the USA in Cuba - the Cuban Missile Crisis. This crisis is generally accepted as the closest that nuclear weapons have come to being used by the USSR and the USA. For more details: Marfleet, B. G. (2000), "The Operational Code of John F. Kennedy during the Cuban Missile Crisis: A Comparison of Public and Private Rhetoric", *Political Psychology*, Vol. 21 (3), p.545; Allison, G. (1969), "Conceptual Models and the Cuban Missile Crisis", *The American Political Science Review*, Vol. 63 (3), pp.689-690; Weldes, J. (1999), *Constructing National Interests: The United States and the Cuban Missile Crisis*, Minneapolis: University of Minnesota Press, pp. 21-23

> *and buck-passing, which can only occur in multipolar worlds, lower system stability."*[202]

In addition to this, Waltz' thesis about the balance of power is that states have to balance policy not against each other, but only against the most powerful states. Whilst the Cold War system could be defined as bipolar, post the Cold War, as new states and new powers emerged, the international community became a multipolar system. Waltz argued that international structure and conflict is now based on the anarchic and decentralized nature of international politics, but this anarchy is not identified by chaos, destruction, or death. The distinction between anarchy and government cannot be explained if anarchy is identified using its accepted meaning.[203] According to Waltz, domestic political structures have a centre, which means that states have their own governmental institutions and offices or units which direct the rules of the state in the territory. Taking this definition of the domestic structure and hierarchy, Waltz explains anarchy as an *"absence of the international government"*,[204] but he believes that international organisations cannot fulfil this role, because national leaders do not want to hand over their power and state sovereignty to another power, suggesting that international organisations may have no more that limited influence on international agreements.[205] Waltz also discusses the self-help system, which asserts that states must defend themselves against outside threats, each community/states or institution having a duty to protect its citizens from any threat.[206] Waltz and other structural neorealist scholars define a threat as having a power asymmetric function.[207] It can be suggested that this function is similar to those espoused by Hobbes and Thucydides, which as previously outlined, provides that if a state has greater power than neighbouring states, the weaker states may feel threatened, because nothing in an anarchic international system hinders the strong state using its power against a weaker neighbour to resolve a conflict.[208] According to Neorealist Theory having international alliances in this period is essential, in order to provide a balance the

[202] Rousseau, (2006), *op.cit.*, p.22

[203] Waltz, K. N. (1979), *The Anarchic Structure of World Politics*, Available at: http://people.reed.edu/~ahm/Courses/Reed-POL-372-2011-S3_IEP/Syllabus/EReadings/01.2/01.2.Waltz2005The-Anarchic.pdf (Accessed at: 10/08/2012), p. 103; Trachtenberg, M. (2003), "The Question of Realism: A Historian's View", *Security Studies*, Vol. 13 (1), p. 157

[204] Waltz, *Ibid*., p. 32; Fox, W. T. R. (1959), "The Uses of International Relations Theory", in Fox, W. T. R. (ed.) (1959), *Theoretical Aspects of International Relations*, Notre Dame: University of Notre Dame Press, p.35

[205] Bordner, B. (1997), *Rethinking Neorealist Theory: Order Within Anarchy*, Available at: http://www.brucebordner.com/Neorealism.html (Accessed at: 12/08/2012)

[206] Waltz (1979), *op.cit.*

[207] Gulick, E. V. (1955), *Europe's Classical Balance of Power*, New York: Norton. Doyle (1997), *op.cit.*, p. 168. Rousseau (2007), *op.cit.*, p.746

[208] Rousseau (2006), *op.cit.* ; Rousseau (2007), *Ibid.* ; Waltz (1979), *op.cit.*

power. However, these alliances are not permanent; because today's friend may be tomorrow's enemy in a war, and therefore these are temporary coalitions.[209]

Stephen Walt explains the balance of threat theory as, "*States form alliances primarily to balance against threats. Threats, in turn, are a function of power, geographic proximity, offensive capabilities, and perceived intentions. Throughout the Cold War, the Soviet Union posed a greater threat to the major powers of Eurasia than the United States did. As "balance-of-threat" theory predicts, these states balanced by allying with the United States, creating a global coalition that was both remarkably stable and significantly stronger than the Soviet alliance network.*" [210] Walt's threat theory is a function of military power, geographical proximity, offensive capability and aggressive intentions.[211] Waltz specifically points to the combination of the balance of power among states, and how these depend on their capabilities in the following areas: *"size of population and territory, resource endowment, economic capability, military strength, political stability and competence".*[212] He states that power is a mixture of all these capabilities, but he also accepted that it was not possible to count them all definitively.

Walt and Waltz strongly support the idea of balance of power theory as more common than bandwagoning, [213] Walt defines 'bandwagoning' as an "*alignment with the source of danger".*[214] Waltz defines bandwagoning as an opposite of the balance. According to him, "*bandwagoning and balancing behaviour are in sharp contrast".*[215] If states join the stronger side, this coalition can be termed 'bandwagoning', rather than 'balancing', but if states join the weaker side to protect their position in the system, this can be termed 'balancing'.[216] Schweller's ideas are opposite to those of Walt and Waltz's ideas. Schweller believes that bandwagoning is more common than Walt and Waltz suggest.[217] Schweller argues that "*the aim of balancing is self-preservation and the protection of values already possessed, while the goal of bandwagoning is usually self-extension: to obtain values coveted. Simply put,*

[209] Grieco J. M. (1988), "Anarchy and the Limits of Cooperation: A Realist Critique of The Newest Liberal Institutionalism", *International Organisation*, Vol. 42, p. 487; Rousseau (2007), *Ibid.*

[210] Walt, *op.cit*., p.vi

[211] *Ibid.*, p.5

[212] Waltz (1979), *op.cit*., p.131

[213] Walt, *op.cit*., p. 5; Waltz, *Ibid*., p. 126; Danilovic, V. (2002), *When the Stakes Are High: Deterrence and Conflict Among Major Powers*, USA: University of Michigan Press, pp. 74-75

[214] *Ibid*., p. 17

[215] Waltz (1979), *op.cit*., p.126

[216] *Ibid*.

[217] Danilovic, *Ibid*.; Schweller, R. L. (1994), "Bandwagoning for Profit: Bringing the Revisionist State Back In", *International Security*, Vol. 19 (1), Available at: http://home.sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/17/Bandwagoning%20for%20Pofits.pdf (Accessed at: 22/05/2016), p. 93

balancing is driven by the desire to avoid losses; bandwagoning by the opportunity for gain."[218] Schweller goes on, "*the purpose of balancing behavior is to prevent systemic disequilibrium or, when deterrence fails, to restore the balance. Balancing is a form of negative feedback. This is not to suggest that bandwagoning effects are always undesirable; this depends on the nature of the existing order. If it is characterized by conflict, bandwagoning behavior may enhance the prospects for a more durable peace. In this regard, the bandwagon's raison d'etre also matters… also balancing is an extremely costly activity that most states would rather not engage in, but sometimes must to survive and protect their values. Bandwagoning rarely involves costs and is typically done in the expectation of gain*."[219] On the other hand, Walt states that balancing is more common than bandwagoning because, he explains, "*states are more secure, because aggressors will face combined opposition. But if bandwagoning is the dominant tendency, then security is scarce, because successful aggressors will attract additional allies, enhancing their power while reducing that of their opponents*."[220] Walt is right in his idea of balancing, because when we think about the Cold War era, states allied with both sides to balance each other. Although Schweller explains bandwagoning only in an economic sense for gain and profit, security and international security are more important than profit, because, as Walt infers where states are trying to maintain their position in the system "*security is the highest end. Only if survival is assured can states safely seek such other goals as tranquillity, profit, and power. Because power is means and not an end, states prefer to join the weaker of two coalitions*."[221] As Schweller states balancing are important to prevent systemic disequilibrium, and therefore the Cold War era is an excellent example of the balance of power theory.

Whilst the focus of this section is NATO's threat perceptions and strategic concepts during the Cold War, the theories of Waltz and Walt go some way to explain international structures both during and post-Cold War. During the Cold War NATO's strategic concepts and policy decisions were based on the balance of power, seeking to explain the idea of mutually assured destruction, with both sides having a large amount of armaments capable of exterminating each other. According to Walt, "*throughout the Cold War, the Soviet Union posed a greater threat to the major powers of Eurasia than the United States did. As 'balance-of-threat' theory predicts, these states balanced by allying with the United States, creating a global*

[218] Schweller, *Ibid.*, p. 74
[219] *Ibid.*
[220] Walt, *op.cit.*, p. 17
[221] Waltz (1979), *op.cit.*, p. 126

coalition that was both remarkably stable and significantly stronger than the Soviet alliance network."[222]

As previously discussed, NATO produced its first strategic concept in 1949. Following some structural changes to the organisation, such as Greece and Turkey joining the Secretary General approved a new strategic concept in 1952, which was called M.C. 3/5.[223] This document superseded the first strategic concept, but echoed the core principles contained in the D.C. 6/1 document which was published by North Atlantic Defense Committee in 1949, because the strategic concept of NATO still saw the USSR the major threat, which determined the strategic concepts of the organisation and the need for collective defence.

At the same time, NATO produced a new strategic guide, in which M.C. 14, D.C. 13 and D.C. 6/1 were revised by the document, M.C. 14/1.[224] The main aim of the organisation was laid out in this document:

> *"In cooperation with any Middle East defence organisation that may be established, [the aim] is to ensure the defence of the NATO area and to destroy the will and capability of the USSR and her satellites to wage war, initially by means of an air offensive, while at the same time conducting air, ground and sea operations designed to preserve the integrity of the NATO area and other areas essential to the prosecution of the war. In the Far East the strategic policy will be defensive."*[225]

The guidance also allowed the organisation to use of all types of weapons against the USSR and its satellites. In 1957 the North Atlantic Military Committee produced another strategic concept, M.C. 14/2. Nuclear weapons were specifically discussed. The nuclear power of the USSR was understood to be targeted against NATO. Massive retaliation was the key strategic response that was identified by the Committee.[226] [227]

In 1968 The Military Committee published, 'Measures to Implement the Strategic Concept' which contained the last strategic concept of the Cold War, which was used until the collapse of the USSR signalled the end of the Cold War. In this document, the USSR was again

[222] Walt, *op.cit*.

[223] The Secretary of the NATO (1952), *M.C.* 3/5 *The Strategic Concept for the Defence of the North Atlantic Area*, Available at: http://www.nato.int/docu/stratdoc/eng/a521203a.pdf (Accessed at: 06/08/2012)

[224] North Atlantic Military Committee (1952), *M. C. 14/1 Strategic Guidance for North Atlantic Regional Planning,* Available at: http://www.nato.int/docu/stratdoc/eng/a521209a.pdf (Accessed at:06/08/2012)

[225] *Ibid*., p.10

[226] Military Committee (1957), *M.C. 14/2 Overall Strategic Concept for the Defense of The North Atlantic Treaty Organisation Area*, Available at: http://www.nato.int/docu/stratdoc/eng/a570523a.pdf (Accessed at: 06/08/2012)

[227] Military Committee (1957), *Measures to Implement the Strategic Concept,* Available at: http://www.nato.int/docu/stratdoc/eng/a570523b.pdf (Accessed at: 07/08/2012)

identified as a major threat that would also use its power in other areas where NATO had some weaknesses, such as economics, politic subversion and military power. The strategic focus of the document was the flexibility and escalation of NATO's policies. According to defence principles, flexibility is defined as:

> *"A flexibility which will prevent the potential aggressor from predicting with confidence NATO's specific response to aggression, and which will lead him to conclude that an unacceptable degree of risk would be involved regardless of the nature of his attack."*[228]

Other significant developments included the Strategic Arms Limitation Talks,[229] known as SALT, between the USA and the Soviet Union. The main aim of these agreements was to reduce and limit nuclear weapons in the international arena.[230] As part of SALT, both sides of the Cold War met to discuss the reduction of weapons, which meant that the Cold War was getting 'softer' and threat perceptions were decreasing. It is also worth noting that during the Cold War whilst NATO's threat perceptions were focussed on the USSR these were not the only threats to international peace and security: terrorism, regional conflict and genocide all presented challenges to the international community.

The next part will examine threat perceptions after the Cold War within NATO's strategic concepts, using some examples. In the last part of the chapter, these threat perceptions will be evaluated within international law and agreements, and consideration will be given as to how the international community has tried to prevent some threats in the international arena.

2.4. The Changing Nature of Security: From Threat to Risk

2.4.1. The Concept of Risk

The concept or notion of risk has become one of the key concepts since the Cold War. With the Strategic Concept of NATO in 1991, the concept of risk has been used instead of the concept of threat. Therefore, it is important to know what the risk is to understand the concept in detail.

[228] Military Committee (1968), *M.C. 14/3 Overall Strategic Concept for the Defense of The North Atlantic Treaty Organisation Area,* Available at: http://www.nato.int/docu/stratdoc/eng/a680116a.pdf (Accessed at:07/08/2012)

[229] The Negotiations began in Helsinki in 1969. These negations were bilateral and about the control of the armament in the area. There were two different agreements, known as SALT 1 and SALT II. SALT II was not ratified by the USA because of the invasion of Afghanistan by the Soviet Union.

[230] For more information: Smart, I. (1970), "The Strategic Arms Limitation Talks", *The World Today*, Vol. 26 (7); Department of State, *Strategic Arms Limitation Talks*, Available at: http://www.state.gov/www/global/arms/treaties/salt1.html (Accessed at: 10/08/2012)

Luhmann states that the concept of risk first appeared between the late Middle Ages and the early modern era.[231] According to Luhmann, the etymology of risk is unknown, the word appearings in Europe in the mid-16th century in German, and in the second half of the 17th century in English.[232] Also he notes that "*the Renaissance Latin term risicum had been in use long before, in Germany as well*."[233] Giddens, on the other side, states that "*the idea of risk, interestingly, was first used by Western explorers when they ventured into new waters in their travels across the world.*"[234] Ewald contends that the concept of risk was first used in the Middle Ages for maritime insurance, to designate the perils that could compromise a successful voyage: "*At that time, risk designated the possibility of an objective danger, an act of God, a force majeure, a tempest or other peril of the sea that could not be imputed to wrongful conduct.*"[235] The concept of risk was accepted as a natural event. Ewald mentions specified natural events, such as "*storms, hail floods, epidemics among animals, fires, and so forth-and excluded damages caused by human beings"*.[236] Lupton states that "*humans could do little but attempt to estimate roughly the likelihood of such events happening and take steps to reduce their impact"*.[237] This idea was to reduce the impact of the natural events and take some measures to reduce the ensuing catastrophe.

According to Lupton, both the meaning and use of the concept of risk changed with the emergence of modernity.[238] Modernity is defined by Giddens as, "*the institutions and modes of behaviour established first of all in post-feudal Europe, but which in the twentieth century increasingly have become world historical in their impact. 'Modernity' can be understood as roughly equivalent to 'the industrialized world', so long as it be recognized that industrialism is not its only institutional dimension. I take industrialism to refer to the social relations implied in the widespread use of material power and machinery in production processes. As such, it is one institutional axis of modernity. A second dimension is capitalism, where this term means a system of commodity production involving both competitive product markets and the commodification of labour power. Each of these can be distinguished analytically from the institutions of surveillance, the basis of the massive increase in organisational*

[231] Luhmann, p. 9

[232] *Ibid*.

[233] *Ibid*

[234] Giddens, A. (1998), "Risk Society: The Context of British Politics", in Franklin, J. (ed.) (1998), *The Politics of Risk Society,* Cambridge: Polity Press, p. 27

[235] Ewald, F. (1993), "Two Infinities of Risk", in Massumi, B. (1993), *The Politics of Everyday Fear,* Minneapolis: University of Minnesota Press, p. 226

[236] *Ibid*., p. 226

[237] Lupton, D. (2013), *Risk*, Oxon: Routledge, p. 5

[238] *Ibid*.

power associated with the emergence of modern social life. Surveillance refers to the supervisory control of subject populations, whether this control takes the form of 'visible' supervision in Foucault's sense, or the use of information to coordinate social activities."[239] Lupton's idea is similar to Giddens, for example, Lupton states that "*modernity is equivalent to the 'industrialized world', incorporating capitalism, the institutions of surveillance and nuclear weaponry as well as the process of industrialism. Modernity depends upon the notion of Enlightenment, emerging in the seventeenth-century, that the key to human progress and social order is objective knowledge of the world through scientific exploration and rational thinking. It assumes that the social and natural worlds follow laws that may be measured, calculated and therefore predicted*."[240] According to the above comments, it can be said that the formation of new modern ideas and modernity began with the Enlightenment, and Martinelli states that the Reformation also had a remarkable effect on modernity and modern ideas. According to Martinelli: "*A subsequent fundamental passage is represented by the Reformation which stressed the conception of the person as an individual. In the teachings of Luther and Calvin, the individual was conceived as alone before God, directly responsible for the interpretation and enactment of God's will. The major consequences of these doctrines for the development of modern culture and institutions were, first, the fostering of the notion of the individual agent as 'master of its destiny' which implies the release of the believer from the institutional support and control of the Church; and, second, the sanctioning of the separation between State and Church and of the autonomy of secular activity in all domains which did not directly conflict with moral and religious practice.*"[241] Modernity, particularly modern ideas, rejected the control of the Church over people, criticizing its role in society, and trying to protect individuals against any restrictions coming from elsewhere.[242] This control system was also seen in political situations, such as the determining role of the Pope on any situation.[243] According to Elmas, the 30 Years' War affected the role of the Pope in the political arena. With the Peace of Westphalia in 1648, the nation-state model increased and the influence of the Church on politics decreased.[244] Martinelli explains that "*the nation-state is the institutional embodiment of political authority*

[239] Giddens, A. (1991), *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Stanford: Stanford University Press, pp. 14-15

[240] Lupton, *op.cit*., pp. 5-6

[241] Martinelli, A. (2005), *Global Modernization: Rethinking the Project of Modernity*, London: SAGE Publications, p. 6

[242] Elmas, S. (2013), *Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik,* Ankara: USAK Yayınları, p. 91

[243] *Ibid*., p. 93

[244] *Ibid*.

in modern society, an impersonal and sovereign political entity with supreme jurisdiction over a clearly delimited territory and population, claiming a monopoly of coercive power, and enjoying legitimacy as a result of its citizens' support."[245] It can be said that modern societies include the formation of three different dimensions; the ideology of modern societies being science, economies being capitalism and the nation-state form being their political system.[246]

With change in political and economic systems and ideology, the concept of risk was also evaluated under the umbrella of science. According to Lupton; "*the science of probability and statistics was developed as a means of calculating the norm and identifying deviations from the norm, thus embodying the belief that rationalized counting and ordering would bring disorder under control. These fields were to become important to the modernist technical notion of risk. During the eighteenth century, the concept of risk had begun to be scientized, drawing upon new ideas in mathematics relating to probability*."[247] Beck asks concerning the calculability and precautions involving risk, "*must one not view and assess the past 200 years as a period of continual growth in calculability and precautions in dealing with industrially produced insecurities and destruction? In fact a very promising approach, and one barely explored to date, is to trace the (political) institutional history of evolving industrial society as the conflict-laden emergence of a system of rules for dealing with industrially produced risks and insecurities.*"[248] He goes on "*its origin go back to the beginnings of intercontinental navigation, but with the growth of industrial capitalism, insurance was continually perfected and expanded into nearly all problem areas of social action. Consequences that at first affect only the individual become 'risks', systematically caused, statistically describable and in that sense 'predictable' types of events, which can therefore also be subjected to supra individual and political rules of recognition, compensation and avoidance*."[249] With modernity, the concept of risk was extended, the notion of risk covering individuals and accepted as predictable events, according to the insurance system stated by the above scholars. As Lupton states, "*the modernist concept of risk represented a new way of viewing the world and its chaotic manifestations, its contingencies and uncertainties. It assumed that unanticipated outcomes may be the consequence of human action rather than 'expressing the hidden meanings of nature or*

[245] Martinelli, *op.cit*., p. 21
[246] Elmas, *op.cit*., p. 101
[247] Lupton, *op.cit*., p. 6
[248] Beck, U. (1992), " From Industrial Society to the Risk Society: Questions of Survival, Social Structure and Ecological Enlightenment", *Theory, Culture & Society*, Vol. 9 (1), pp. 98-99
[249] *Ibid*., p. 99

ineffable intentions of the Deity', largely replacing earlier concepts of fate or fortune."[250] It may be understood from this that the new meaning of the concept of risk replaced the existing ideas of risk as natural events or acts of God with humanitarian actions and unanticipated outcomes. From the nineteenth century, the notion of risk was evaluated with insurance. Ewald explains this situation as "*the notion of risk is likewise central to the juridical definition of insurance: 'risk is the fundamental element of insurance, since it is the very object of this type of contract'. Risk constitutes an essential element of insurance; the fundamental element, even, for Picard and Besson who add: 'this notion of risk is specific in its origin to the law and science of insurance, and differs markedly from the notion of risk utilised in civil law and everyday speech*'."[251] In the nineteenth century, the concept of risk was developed in insurance, and Ewald's idea supported the concept of the evaluation of the notion of risk along with insurance. According to Ewald, "*the notion of risk goes together with those of chance, hazard, probability, eventuality or randomness on the one hand, and those of loss or damage on the other- two series coming together in the notion of accident. One insures against accident, against the probability of loss of some good. Insurance, through the category of risk, objectifies every event as an accident. Insurance's general model is the game of chance; a risk, an accident comes up like a roulette number, a card pulled out of a pack. With insurance, gaming becomes a symbol of the world*."[252] From here it can be understood that risk was divided into two different categories, as good or bad risk, or losses or gains.[253] It seems clear that the understanding of risk was based on the losses or gains in the nineteenth century, and the marine insurance or the concept of insurance developed with the notion of risk. The meaning of risk changed in the twentieth century, and Douglas states that "*the notion of risk has come to the politics because the probabilistic thinking is pervasive in industry, modern science, and philosophy. Risk would have become the idiom of politics as part of the homogenizing process of moving to a new world level of*

[250] Lupton, *op.cit.*, pp. 6-7

[251] Ewald, F. (1991), "Insurance and Risk", in Burchell, G. Gordon, C. and Miller, P. (eds.) (1991), *The Foucault Effect: Studies in Governmentality*, London: Harvester, p. 199

[252] *Ibid.*

[253] For example, Douglas writes about the concept of risk as "the chances of a ship coming safely home and making the fortune of its owner were set against the chances of its being lost at sea, bringing ruin. The idea of risk in itself was neutral; it took account of the probability of losses and gains. Going further back still, the concept originally emerged in the seventeenth century in the context of gambling. For this purpose a specialized mathematical analysis of chances was developed. Risk then meant the probability of an event occurring, combined with the magnitude of the losses or gains that would be entailed. Since the seventeenth century the analysis of probabilities has become the basis of scientific knowledge, transforming the nature of evidence, of knowledge, of authority, and of logic. Any process or any activity has its probabilities of success or failure. The calculation of risk is deeply entrenched in science and manufacturing and as a theoretical base for decision-making." Douglas, M. (1992), *Risk and Blame: Essays in Cultural Theory*, London: Routledge, p. 23

interaction. However, the risk that is a central concept for our policy debates has not got much to do with probability calculations. The original connection is only indicated by arm-waving in the direction of possible science: the word risk now means danger; high risk means a lot of danger."[254] It seems clear that the probability of risk changed from nineteenth century to twentieth century. As Douglas states, risk was accepted as good or bad/ losses or gains, but as Ewald mentions, "*risk is now generally used to relate only to negative or undesirable outcomes, not positive outcomes".*[255] Also, Rowe's definition of the notion of risk supports the idea of Ewald as *"the potential for realization of unwanted, negative consequences of an event*."[256]

The nature of the concept of risk has changed over time. With the evaluation of the notion of risk, states and international organisations have used the term to identify their security policies. As explained previously, the concept of threat was directly used in Cold War term, but after the Cold War, the notion of risk is used to refer to any situation against peace and security. Also it must be mentioned here that the concepts of threat and risk are different. Earlier definition explains this situation clearly, but Williams explains differences between threat and risk as: "*whereas threat is quantifiable because of assessment in terms of capabilities which one either possesses or not, risk is not nearly as computable.*"[257] This explanation illustrates the differences between the Cold War period and the Post-Cold War period, because there was a visible threat posed by the USSR during the Cold War, but, since then, there have been unpredictable risks in the world. Therefore, NATO's first strategic concept after the Cold War mentioned the concept of risk rather than the concept of threat.

It is difficult to perform true risk assessment, because no one knows the effect of risk, as compared with threat. As Heng states, "*threat was defined largely by notions of military power, power-resources and means of power rightly or wrongly perceived as overwhelming or not. Without power, there will be no threat…A new paradigm based on risk would in contrast revolve not on power capabilities and intentions but rather dangers considered at the level of their potentiality and probable magnitude of consequences. Dangers now stem not from powerful states but failed and destabilised states posing risks through globalisation, terrorist and refugee flows, or diseases. These dangers are conceptualised as risks in terms of their probabilities and consequences, since their material power capabilities or intent are*

[254] *Ibid*., pp. 23-24

[255] Lupton, *op.cit*., p. 8

[256] Tierney, K. T. (1999), "Toward a Critical Sociology of Risk", *Sociological Forum*, Vol. 14 (2), Available at: http://www.jstor.org/stable/pdf/684794.pdf?_=1466111013813 (Accessed at: 15/06/2016), p. 217

[257] Williams, M. J. (2008), "(In) Security Studies, Reflexive Modernization and the Risk Society", *Cooperation and Conflict: Journal of the Nordic International Studies Association*, Vol. 43 (1), p. 65

impossible to gauge or even non-existent."[258] From this statement, it can be said that the concept of risk covers probabilities and consequences, while on the other hand, the concept of threat involves power capabilities and the notion of power in general. Also, Williams states, "*since at least the founding of the modern states system at Westphalia in 1648, the idea of threat has relied on another's capabilities and intentions coupled with one's own inference of the possible threat. Threat relies explicitly on an 'other'. If there is no other, then there can be no threat. The same is not true of risk. Risk can be perceived independent of an identifiable actor.*"[259] Williams' idea supports Heng's statement in terms of different points of the concepts of threat and risk. Also, as Williams' statement shows, threat could be acceptable when there is an 'other', but the concept of risk does not need another, and can stem from anywhere, such as from powerful states or failed states.

The concept of risk has been defined, and differences between threat and risk outlined above. Social science risk theories will now be briefly explained and in this regard, the Risk Society will be detailed in a subsequent section to understand NATO's new strategic concept/s.

2.4.1.1. Social Science Approaches to Risk

The main aim of this section is to evaluate sociological risk theories, and, in this regard, to understand and analyse the risk society. There are many different taxonomies on social science approaches to risk. For example, Zinn theorizes the concept of risk according to five different sociological approaches. These are: Risk Society by Ulrich Beck, Governmentality by Foucault, Luhmann's System Theory, Edgework concept by Lyng and lastly, Cultural approach by Douglas.[260]

Renn uses different taxonomies to theorize risk, and although his taxonomy covers many of Zinn's risk taxonomies, Renn's taxonomy is broader than that of Zinn. In this regard, Renn's taxonomy on theories of the concept of risk is used in this thesis.

Renn analyses sociological risk theories in two different dimensions as: Constructivist-Realist and Individualistic-Structural.[261]

[258] Heng, Y. K. (2006), *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, London: Routledge, p. 49

[259] Williams, M. J. (2009), *NATO, Security and Risk Management: From Kosovo to Khandahar*, Oxon: Routledge, p. 18

[260] Zinn, J. O. (2008), *Social Theories of Risk and Uncertainty: An Introduction*, Oxford: Blackwell Publishing, pp. 15-16

[261] He explains these dimensions and why he choices this classification as: "This taxonomy orders sociological approaches with regard to two dimensions: individualistic versus structural, and realist versus constructivist approaches. The major reasons for this classification are as follows:

- The classification is simple and straightforward – and, thus, open to criticism.

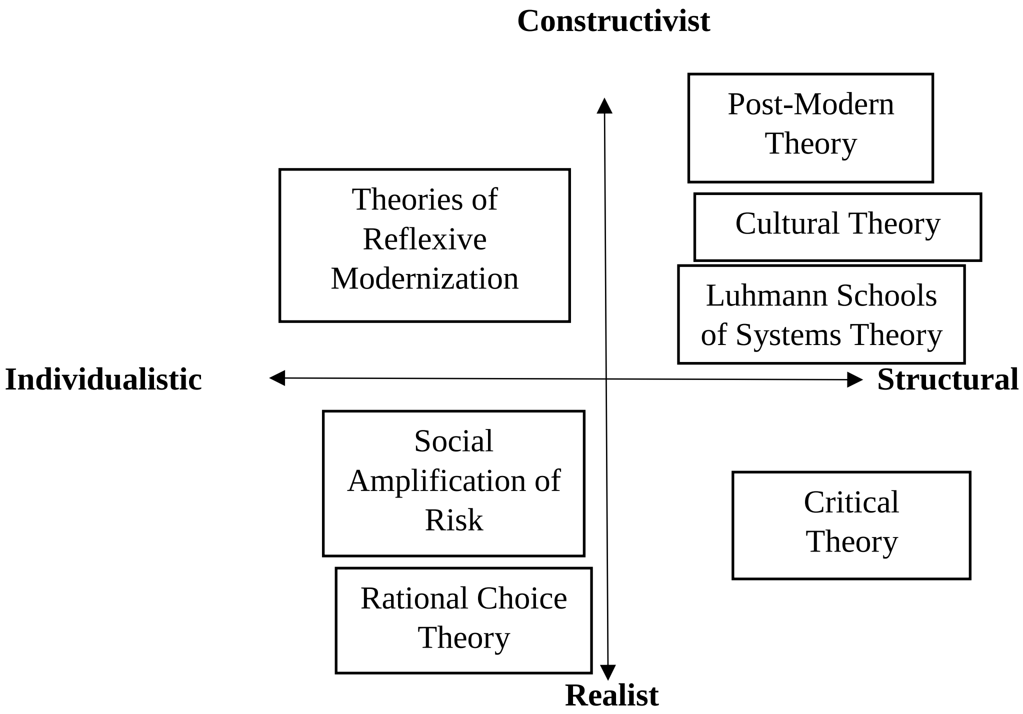

Figure 1: Review of Sociological Approaches to Risk

Renn, O. (2008), *Risk Governance: Coping With Uncertainty in a Complex World*, London: Earthscan, p. 24

It seems clear that Renn analyses the concept of risk in seven different social-based theoretical approaches, which are broader than Zinn's approach. Six different social-based theoretical approaches will be briefly highlighted, and, the main aspect of this section, Risk Society and Reflexive Modernization, will be deeply analysed.

Rational choice theory is based on the decisions of individuals. Individuals are the centre in this approach. According to Renn, "*it parts from the assumption that human beings are*

- The classification fits the overall framework of risk perspectives developed above.
- Most, if not all, social science concepts of risks can be grouped within the boundaries of these two dimensions.
- The two dimensions appear to be sufficient to distinguish between concepts that are clearly distinct from each other.

The two attributes 'individualistic' and 'structural' indicate the base unit of the analysis. The x-axis represents the normative continuum between an individualistic (agency-oriented) and structural (collective) focus when investigating risk debates. It is either focused on the individual or a social aggregate such as an institution, a social group, a subculture or a society. Structural concepts emphasize that complex social phenomena cannot be explained by individual behaviour alone, but that they rest on interactive (often unintentional) effects among individuals and between individuals and institutions. The y-axis represents the continuum between the extreme positions regarding the foundations of knowledge (description). At the top appears the position that all knowledge is socially constructed; at the bottom is the opposite view that all knowledge is, and can be, directly experienced from a physical reality accessible through a combination of data collection and theoretical reasoning. 'Realist' and 'constructivist' concepts differ in their view of the nature of risk and its manifestations. Whereas the objective concept implies that risks and their manifestations are real, observable events, the constructivist concept claims that risk and their manifestations are 'social artefacts' fabricated by social groups or institutions." Renn, O. (2008), *Risk Governance: Coping With Uncertainty in a Complex World*, London: Earthscan, p. 24

capable of acting in a strategic fashion by linking decisions with outcomes."[262] *Many special theories on risk and uncertainty rely on the rational actor paradigm (RAP) concept and its propositions. These propositions refer to human actions based on individual decisions. Among the most important are:*

> *• The atomistic view of rationality (all actions can be reduced to individual choices);*
>
> *• Analytical separation of means and ends (people, as well as institutions, can, in principle, distinguish between ends and means to achieve these ends);*
>
> *• Goal-attainment motivation (individuals are motivated to pursue self-chosen goals when selecting decision options);*
>
> *• Maximization or optimization of individual utility (human actors select the course of action which promises to lead to more personal satisfaction than any other available course of action);*
>
> *• Knowledge about potential outcomes (people who face a decision can make judgements about the potential consequences of their choices and their likelihood);*
>
> *• Human preferences (people have preferences about decision outcomes based on values and expected benefits);*
>
> *• predictability of human actions if preferences and subjective knowledge are known (rational actor theory is not only a normative model of how people should decide, but also a descriptive model of how people consciously or subconsciously select options and justify their actions)".*[263]

It seems clear that individual choices are important in this approach, and human choices with their different decisions affect the subjective expectations. This approach is mostly used in economics, but it can be useful in psychology in terms of determining how individuals choose their decision with regards to their expectations.

Luhmann's system theory understands the concept of risk as a fundamental social construct, and it is linked to the rationalities of social sub-systems.[264] [265] According to Luhmann, these

[262] *Ibid*., p. 25

[263] *Ibid*., pp. 25-26

[264] Renn, O. (2008), *Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts,* Available at: http://docserver.ingentaconnect.com/deliver/connect/oekom/09405550/v17n1/s13.pdf?expires=1466950964&id=87723253&titleid=6690&accname=Guest+User&checksum=72DAC3996A08B9BDFE9ABA7BB50D3BAE (Accessed at: 15/06/2016), p. 59

sub-systems can be seen in modern societies, and communication is the basic element of social operation.[266] By contrast, Luhmann states that if any event or case has a social effect or response, it is accepted as a subject of communication.

> "*But as physical, chemical or biological facts they create no social resonance as long as they are not the subject of communication. Fish or humans may die because swimming in the seas and rivers has become unhealthy. The oil-pumps may run dry and the average climatic temperatures may rise or fall. As long as this is not the subject of communication it has no social effect. Society is an environmentally sensitive (open) but operatively closed system. Its sole mode of observation is communication. It is limited to communicating meaningfully and regulating this communication through communication.*"[267]

Luhmann's system theory puts communication at the centre of social operations. Also, Arnoldi states that communicative systems can reduce the complexity in both de-selecting and forming expectations, observing that Luhmann separates danger and risk.[268] He states that "*dangers are random events while risks are attributable to decisions, to individuals or society having actively (de-)selected and narrowed frames of expectations. Any complexity reduction (i.e. a decision) is risky, but in today's highly complex societies there is even more risk- that is, more pressure to make decisions*."[269] It may be said that the concept of risk is the consequence of any decision, but that the danger that comes from outside can be evaluated, and there is no internal control or decision on it. Rosa emphasises Luhmann, stating that "*in the case of risk, losses that may occur in the future are attributed to decisions made…the concept risk is, however, clearly distinguished from the concept of danger, that is to say, from the case where future losses are seen not all as the consequences of a decision that has been*

[265] Renn states concerning the system theory that "human societies are organized as a variety of self-referential or autopoietic (self-reproducing) systems which define their own reality as well as an image of the world outside. Systems include functional entities such as the law, the economy, and the political hierarchy. All systems and sub-systems have generated special communication media (such as legal codes, money and power) to reduce complexity. These media ensure internal order and provide the necessary exchange with external systems. The sustainability of social systems depends upon the ability to exchange media. Media form the (binary) code of interaction within and between systems." *Ibid*.; See also**;** Renn, O. (2008), "*Risk Governance: Coping With Uncertainty in a Complex World, op.cit.*, p. 31

[266] Luhmann, N. (1989), *Ecological Communication*, Translated by Bednarz, J. (1989), Chicago: The University of Chicago Press, p. 29; Luhmann, N. (1994), *Social Systems*, Translated by Bednarz, J. and Baecker, D. (1995), Stanford: Stanford University Press, p. xii

[267] Luhmann (1989), *Ibid*., pp. 28-29

[268] Arnoldi, J. (2009), *Risk*, Cambridge: Polity Press, p. 62

[269] *Ibid*.

made, but attributed to an external factor. With respect to dangers, however, society faces a problem that the injured party has not himself caused."[270] Like Beck and Giddens, Luhmann accepts that natural events are drawn into the system and therefore the world is going to become more risky. According to Renn, "*the more social systems act to shape the future, the more dangers are internalized and, axiomatically, the more risks are 'created'. For example, changing climate – once thought nature's caprice – is now viewed as significantly shaped by humans and is, therefore, a risk*."[271]

In short, Luhmann's system theory places communication at the centre of social operations, and separates risk and danger. Decision is a key feature in the concept of risk, but, on the other hand, natural or outside events provide the element of danger.[272]

Critical theory; Elmas states that critical theory accepts that the concept of risk is caused by the capitalist system and its institutions and is the reality of the world.[273] Renn also states that "*the critical theory accepts the objective component of the rational actor approach but relies on structural analysis for determining institutional interests and social group behaviour*."[274] Renn explains critical theory in his study as: "*critical theory relies partially on a systems perspective, but assumes an overarching rationality that bridges the different rationalities of the social systems and the institutions in a pluralist society*."[275] It can be understood from this that critical theory supports social cohesion against individuality, and believes that social integration can resolve social problems. Renn also argues that communication is important to resolve the problems of social groups, and therefore the public discussion arena is essential to discuss problems of social nature. Renn continues, "*critical theory, the only viable solution to overcome this imbalance is to create a forum for open discourse, where all actors have the opportunity to argue their interests and where thus conflicts are resolved in an equitable and rational manner. The process of discourse must be fair, transparent, and truthful*."[276] Critical

[270] Rosa, E. A. (2003), "The Logical Structure of the Social Amplification of Risk Framework (SARF): Metatheoretical Foundations and Policy Implications", in Pidgeon, N., Kasperson, R. E. and Slovic, P. (eds.) (2003), *The Social Amplification of Risk,* Cambridge: Cambridge University Press, p. 71

[271] Renn, O. (2008), *Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts, op.cit.,* p. 60

[272] Lidskog and Sundqvist derive from Luhmann that "the cause of the damage could either be attributed to the system itself (risk) or something external to the system (danger)." Lidskog, R., and Sundqvist, G. (2013), "Sociology of Risk", in Roeser, S., Hillerbrand, R., Sandin, P., and Peterson, M. (eds.) (2013), *Essentials of Risk Theory*, London: Springer, p. 91

[273] Elmas, *op.cit*., p. 83

[274] Renn, O. (1992), *Concept of Risk: A Classification*, Available at: https://www.researchgate.net/publication/245760840_Concepts_of_risk_A_classification (Accessed at: 16/06/2016), p. 70

[275] Renn, O. (2008), *Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts, op.cit.,* p. 60

[276] *Ibid*.

theory suggests that if different social groups create common understanding against any case or risks, the problem can resolve, but, on the other hand, if both sides of the social group inflict their own policies, the application and implication of these policies can lead to an unequal place.[277]

Cultural theory has been developed by Douglas and Wildavsky.[278] Douglas explains cultural theory as: "*cultural theory is a way of thinking about culture that draws the social environment systematically into the picture of individual choices*."[279] Cultural theory believes that risk has been instilled into cultural codes and this cannot be explained under physiological behaviours. Risk perceptions can only be explained under social codes which are transferred by ancestry.[280] According to Rippl, "*risk perception and concern about environmental or social issues are socially and culturally framed. This means that the values and worldwides of certain social or cultural contexts shape the individual's perception and evaluation of risks. Douglas and Wildavsky stress that individuals are embedded in a social structure and that the social context of individuals shapes their values, attitudes, and worldwides*."[281] From this explanation, it can be said that individuals' views and common social experiences are parallel.[282]

Douglas also mentions that there are many cultural types for comparison, but only three political types of cultural theory can provide a powerful explanation of attitudes to risk: hierarchical, individualist and sectarian.[283] Besides, Douglas and Wildavsky use grid and group analysis to explain the relation between social organisation and values and beliefs.[284]

[277] Renn states that "the focus is on the normative aspect of emancipation rather than explanation of risk experience or policies for risk reduction. Emancipation in this context involves the empowerment of groups and communities to enable them to determine their own acceptable risk level. According to this perspective, present risk policies suffer a legitimation crisis because they are based on the imposition of risks by one social group on another (reproduction of class structure) and are often not in the interest of those who have to bear them (lack of social integration). The risk experiences by different social groups reflect the class structure of society and indicate the inequities in the distribution of power and social influence." Renn, O. (1992), *op.cit.*, pp. 70-71

[278] Rippl, S. (2002), "Cultural Theory and Risk Perception: A Proposal for a Better Measurement", *Journal of Risk Research*, Vol. 5(2), p. 148; Zinn, *op.cit.*, p. 16

[279] Douglas, *op.cit.*, p. xi

[280] Elmas, *op.cit.*, p. 85

[281] Rippl, *op.cit.*, p. 148

[282] Elmas, *op.cit.*, p.85

[283] Douglas, *op.cit*, p. 47

[284] According to Douglas and Wildavsky: "This is a way of checking characteristics of social organisation with features of the beliefs and values of the people who are keeping the form of organisation alive. Group means the outside boundary that people have erected between themselves and the outside world. Grid means all the other social distinctions and delegations of authority that they use to limit how people behave to one another. A society organized by hierarchy would have many group-encircling and group-identifying regulations plus many grid constraints on how to act. An individualist society would leave to individuals maximum freedom to negotiate with each other, so it would have no effective group boundaries and no insulating constraints on private dealings. A sectarian society would be recognizable by strong barriers identifying and separating the community from non-members, but it would be so egalitarian that it would have no leaders and no rules of

Poel and Fahlquist state that "*Douglas and Wildavsky claim that each bias corresponds to a particular selection of dangers as risks. According to Douglas and Wildavsky, dangers cannot be known directly. Instead they are culturally constructed as risks. Depending on the cultural bias, certain dangers are pre-eminently focused on. Hierarchists focus on risks of human violence (war, terrorism, and crime), market individualists on risks of economic collapse, and sectarians on risks of technology*."[285] On the other side, Nick Fox writes of the grid/group typology of Douglas and Wildavsky as: "*What is considered as a risk, and how serious that risk is thought to be, will be perceived differently depending upon the organisation or grouping to which a person belongs or identifies, as will the disasters, accidents or other negative occurrences which occur in a culture. The free-market environment (low grid and low group) will see competitors as the main risk, to be countered by good teamwork and leadership. In the bureaucratic culture (high grid and high group), the external environment is perceived as generally punitive, and group commitment is the main way to reduce risk. Finally, in the voluntary culture (low grid with high group), the risks come from external conspiracies, and group members may be suspected of treachery*."[286] In short, cultural theory claims that culture draws the framework for the recognizing risks.[287]

Post-Modern Theory; Renn states that the concept of risk is not at the centre of the Post-Modern Theory.[288] Renn explains this situation as, "*Many post-modernists are radical individualists who believe that the individual is able to cope with contingencies and to arrive at the most appropriate balance of expected positive and negative outcomes. However, what is seen as risks and what as benefits, and to what degree, depends upon the framing of social forces*."[289] Also, Elmas accepts that the concept of risk in post-modern theory is the routing instrument for decision-makers who try to achieve social control in a society.[290] Besides,

precedence or protocol telling people how to behave." Douglas, M. and Wildavsky, A. (1982), *An Essay on the Selection of Technological and Environmental Dangers: Risk and Culture*, Berkeley: University of California Press, p. 88

[285] Poel, I. and Fahlquist, J. N. (2013)," Risk and Responsibility", in Roeser, S., Hillerbrand, R., Sandin, P., and Peterson, M. (eds.) (2013), *Essentials of Risk Theory*, London: Springer, pp. 110-111

[286] Fox, N. (1999), "Postmodern Reflections on 'Risks', 'Hazards' and Life Choices", in Lupton, D. (ed.) (1999), *Risk and Sociocultural Theory*, Cambridge: University of Cambridge Press, p. 15

[287] Kasperson and Kasperson states that "culture is the framework by which people recognize risks. The community is the context for the individual's view of the world and the scale of values by which different risk consequences are reckoned grave or trivial." Kasperson, R. E. and Kasperson, J. X. (2005), "Considerations and Principles for Risk Communication for Industrial Accidents", in Kasperson, R. E. and Kasperson, J. X. (eds.) (2005), *The Social Contours of Risk: Publics, Risk Communication and The Social Amplification of Risk*, London: Earthscan, p. 75

[288] Renn, *op.cit.*, p.36

[289] *Ibid*.

[290] Elmas, *op.cit.*, p. 85

post-modern theory does not accept objective reality, and Renn indicates that "*independent of the question of whether an objective reality exists, post-modernists believe that all claims towards an objective world are guided by personal interests and group-specific reasoning. They are interested in revealing the hidden power motives behind claims of individuals and groups to enforce behavioural, moral or cognitive norms on others. Risks are part of this game to legitimize power.*"[291] Fox's opinion is similar to that of Renn. Lupton quoted from Fox that "*risks and hazards are regarded as social constructions. From this position, hazards may be understood as the reifications of moral judgements about the 'riskiness' of choices, evoked discursively to support estimations of risk and those assessed to be 'at risk'. Fox examines the life choices made by people in relation to risk using two case studies: the first of health in the workplace and the second of drug use in club culture. He argues that assessing environmental circumstances as 'risks' masks political claims about how people should live, silencing voices which dissent.*"[292] When we compare Renn's and Fox's ideas, Elmas is right in his explaining of the concept of risk in post-modern theory as a routing instrument. In addition, Lupton uses Foucault's governmentality concept to explain the role of risk in liberal government.[293]

In short, it can be said that the concept of risk in post-modern theory has been used in the community to constitute social control, the framing of which is important in the post-modern theory of risk.

Social Amplification of Risk Framework (SARF) was proposed by Kasperson and his colleagues in 1988.[294] Pidgeon *et al* state that SARF "*aims to examine broadly, and in social*

[291] Renn, *op.cit.*, p. 35

[292] Lupton, op.cit., p. 7

[293] "Foucault and exponents of the 'governmentality' perspective have described, a huge network of expert knowledges has developed, accompanied by apparatuses and institutions built around the construction, reproduction, dissemination and practice of these knowledges. This is an outcome of the emergence of the modern system of liberal government, with its emphasis on rule and the maintenance of order through voluntary self-discipline rather than via coercive or violent means. Risk is understood as one of the heterogeneous governmental strategies of disciplinary power by which populations and individuals are monitored and managed so as to best meet the goals of democratic humanism. Normalization, or the method by which norms of behaviour or health status are identified in populations and by which individuals are then compared to determine how best they fit the norm, is a central aspect of liberal government. Those who are determined to deviate from the norm significantly are typically identified as being 'at risk'. To be designated as 'at risk', therefore, is to be positioned within a network of factors drawn from the observation of others." *Ibid.*, pp. 4-5

[294] Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X., and Ratick, S. (1988), "The Social Amplification of Risk: A Conceptual Framework", *Risk Analysis*, Vol. 8 (2), p. 179; Renn, O., Burns, W. J., Kasperson, J. X., Kasperson, R. E. and Slovic, P. (1992), "The Social Amplification of Risk: Theoretical Foundations and Empirical Applications", *Journal of Social Issues*, Vol. 48 (4), p. 139; Pidgeon, N., Kasperson, R. E. and Slovic, P. (eds.) (2003), *The Social Amplification of Risk*, Cambridge: Cambridge University Press, p. 2; Zinn, J. O. and Taylor-Gooby, P. (2006), "Risk as an Interdisciplinary Research Area", in Taylor-Gooby, P. and Taylor-Gooby, P. (eds.) (2006), Risk in Social Science, Oxford: Oxford University Press, p. 32

and historical context, how risk and risk events interact with psychological, social, institutional, and cultural processes in ways that amplify or attenuate risk perceptions and concerns, and thereby shape risk behaviour, influence institutional processes, and affect risk consequences."[295] It seems clear that SARF examines and analyses the concept of risk among different disciplines. This means that SARF has an important part to play, because other concepts, such as psychology or sociology, analyse the concept separately, which means that each discipline has its own risk analysis, whereas SARF analyses the concept of risk with the eyes of different disciplines.[296]

According to Kasperson *et al* "*amplification occurs at two stages: in the transfer of information about the risk, and in the response mechanisms of society. Signals about risk are processed by individual and social amplification stations, including the scientist who communicates the risk assessment, the news media, cultural groups, interpersonal networks, and others. Key steps of amplifications can be identified at each stage. The amplified risk leads to behavioural responses, which, in turn, result in secondary impacts*."[297] Social interactions can affect the interpretation of signals, and this situation can create risk amplification or risk attenuation. The secondary stage or impacts will be spawned in response to the interpretation of risk signals.[298] Slovic gives September 11 as an example of secondary stage effects on social disorder.[299] In short, Renn states that "*the experience of risk is not an experience of physical harm, but the result of a process by which individuals or groups learn to acquire or create interpretations of hazards. These interpretations provide rules of how to select, order, and often explain signals from the physical world*."[300] In short, interpretation and social interaction are important for risk assessment. This interpretation will create risk amplification or risk attenuation.

[295] Pidgeon *et al.* (2003), *Ibid*., p.2

[296] Kasperson, J. X. and Kasperson, R. E. (eds.) (2005), *The Social Contours of Risk Volume 2: Risk Analysis, Corporations & the Globalization of Risk*, London: Earthscan, p. 10

[297] Kasperson *et al.* (1988), *op.cit*., p 177

[298] According to Kasperson et al secondary stage includes effects such as:
" -Enduring mental perceptions, images, and attitudes (e.g., anti technology attitudes, alienation from the physical environment, social apathy, stigmatization of an environment or risk manager);
-Local impacts on business sales, residential property values, and economic activity;
-Political and social pressure (e.g., political demands, changes in political climate and culture); Changes in the physical nature of the risk (e.g., feedback mechanisms that enlarge or lower the risk);
-Changes in training, education, or required qualifications of operating and emergency response personnel;
-Social disorder (e.g., protesting, rioting, sabotage, terrorism);
-Changes in risk monitoring and regulation;
-Increased liability and insurance costs;
-Repercussions on other technologies (e.g., lower levels of public acceptance) and on social institutions (e.g., erosion of public trust)." *Ibid*., p. 182

[299] Slovic, P. (2002), "Terrorism as Hazard: A New Species of Trouble", *Risk Analysis*, Vol. 22(3), p. 426

[300] Renn *et al.* (1992), *op.cit*., p. 140

The next heading, Risk Society and Reflexive Modernization, will now be analysed, and NATO's new concepts and its new role will be evaluated in accordance with the risk society and reflexive modernization.

2.4.1.2. Risk Society and Reflexive Modernization

The concept of risk society was developed by Ulrich Beck and Anthony Giddens. Beck states that the concepts of risk and of risk society are side effects from our industrialized way of life, or in other words, from modernity.[301] Sorensen and Christiansen mention that "*the risks are unintended side effects: side effects that could not have been planned for, are not wanted or needed and could not have been predicted. They simply appeared wherever industrial society turned out to be prosperous and successful.*"[302] The concept of risk is a product of modern life and concerns incidents affecting the future. Beck states that "*risks concern the possibility of future occurrences and developments; they make present a state of the world that does not (yet) exist.*"[303] Mythen suggests that a risk in the risk society is not one that is happening now, but may happen in the future.[304] He interprets Ewald's ideas that "*in modern discourse, risk relates to a desire to control and predict the future: "To calculate a risk is to master time, to discipline the future. To provide for the future does not just mean living from day to day and arming oneself against ill fortune, but also mathematizing one's commitment.*"[305] From these statements, it can be said that the risk society is a criticism of modernity, and that prediction is essential to save the future of the world.

As mentioned previously, modern society includes three different dimensions, the ideology of modern societies being science, capitalism and the formation of the nation-state.[306] On the other hand, risk society argues over these three principles, Elmas stating that risks have more advantages than disadvantages. Abbott *et al* articulate that the nuclear accident in Chernobyl in 1986 was an example of the characteristic of a risk society.[307] They continue, "*the consequences of the incident are indeterminate, the causes complex and future developments*

[301] Sorensen, M. P. and Christiansen, A. (2013), *Ulrich Beck: An Introduction to the Theory of Second Modernity and the Risk Society*, London: Routledge, p. 22
[302] *Ibid*.
[303] Beck, U. (2009), *World at Risk*, Cambridge: Polity Press, p. 9
[304] Mythen, G. (2004), *Ulrich Beck: A Critical Introduction to the Risk Society*, London: Pluto Press, p. 14
[305] *Ibid*.
[306] Footnote 247
[307] Abbott, P., Wallace, C. and Beck, M. (2006), "Chernobyl: Living with Risk and Uncertainty", *Health, Risk& Society*, Vol. 8 (2), Available at: https://www.abdn.ac.uk/socsci/documents/AWB2006.pdf (Accessed at: 15/07/2016), p. 105

unpredictable."[308] Zinn states that the nuclear power catastrophe in Chernobyl was an indicator of the safety situations of technologies and the ability of states to control these large-scale technologies.[309] Modernity advocates that social life is guaranteed within the nation-state border under public information supervision, control and assurance.[310] On the other hand, according to risk society, modern industrialized nations have lost their legality in terms of guaranteeing public information supervision, control and assurance, because with the Chernobyl catastrophe, risks within these borders were not under control.[311] Renn explains this situation as: "*the theory of reflexive modernization rests on the assumption that the meta-rationality of modernity (i.e. instrumental rationality, efficiency, justice through economic growth, and steady improvement of individual living conditions through scientific and technical progress) has lost its legitimizing power*."[312] Also, Beck states that the risks which come from the industrialized world cannot be brought under control and are now influential in the wide geography.[313]

Beck separates the concept of risk into two different stages:

> *"In the first instance, risk seems no more than a part of an essential calculus, a means of sealing off boundaries as the future is invaded. Risk makes the unforeseeable, or promises to do so. In this initial form, risk is a statistical part of the operation of insurance companies. They know a lot about the secrets of risk which change society, even though nothing has yet happened. This is risk in a world where much remains as 'given', as fate, including external nature and those forms of social life coordinated by tradition. As nature becomes permeated by industrialization and as tradition is dissolved, new types of incalculability emerge. We move then into the second stage of risk, which Giddens and I have called manufactured uncertainty. Here the production of risk is the consequence of scientific and political efforts to control or minimize them."*[314]

The division of risk into stages can only be explained by criticism of modernity, because the first stage of risk can come from anywhere which does not enjoy the effects of modernity; on

[308] *Ibid*.
[309] Zinn, *op.cit*., p.
[310] Elmas, *op.cit*., p. 104
[311] *Ibid*.
[312] Renn (2008), *Risk Governance…*, *op.cit*., p. 27
[313] Beck, U. (1992), *Risk Society: Towards a New Modernity*, London: SAGE Publications, p. 13
[314] Beck, U. (1998), Politics of Risk Society, in Franklin, J. (1998), *The Politics of Risk Society*, Cambridge: Polity Press, p. 12

the other hand, the second stage of risk is produced by people and modernity. Modern societies try to control risks or threats, but Beck states that they aid the concept of risk in terms of improvement,[315] and therefore modern societies are faced with the unintended side effects of modernity.[316]

Moreover, Beck separates modernity into two different stages: simple modernity and reflexive second modernity.[317] According to Lash, the structure of society is linear, and there is equilibrium in the simple/first modernity.[318] The risks can only come from external elements and the system only changes with these external forces.[319] On the other hand, the changes in the second modernity begin with the degradation of the system layouts when the system itself is questioned, and tries to take measures to protect itself.[320] Beck explains the differences between first and second modernity: "*the driving force in the class society can be summarized in the phrase: I am hungry! The movement set in motion by the risk society, on the other hand, is expressed in the statement: I am afraid! The commonality of anxiety takes the place of the commonality of need.*"[321] It seems clear that there is a strong difference between first and second society, because industrialization and technological development have created a fear in society, as these developments are not only used for social aims; they are also used by terrorists to inflict on society. Beck also states in his work that "*modernization is becoming reflexive; it is becoming its own theme. Questions of the development and employment of technologies (in the realms of nature, society and the personality) are being eclipsed by questions of the political and economic management of the risks of actually or potentially utilized technologies-discovering, administering, acknowledging, avoiding or concealing such hazards with respect to specially defined horizons of relevance. The promise of security grows with the risks and destruction and must be reaffirmed over and over again to alert and critical public through cosmetic or real interventions in the techno-economic development.*"[322] Beck is right in his ideas, because developments in technology and economy, states and society may result in prosperity, but on the other hand, they may also create new risks for society, such as cybercrime and cyber

[315] Ibid., pp. 10-12

[316] Sorensen (2013), *op.cit.*, p. 23

[317] Beck, U., Bonss, W. And Lau, C. (2003), "The Theory of Reflexive Modernization: Problematic, Hypotheses and Research Programme", *Theory, Culture&Society*, Vol. 20 (1), p. 2

[318] Lash, S. (2003), "Reflexivity as Non-Linearity", *Theory, Culture&Society,* Vol. 20 (2), p. 50

[319] *Ibid*.

[320] Elmas, *op.cit*., p. 110

[321] Beck (1992), *op.cit*., p. 49

[322] *Ibid*., pp. 19-20

terrorism. Technological developments can be used by terrorists or hackers for their own aims.

Elmas states that reflexive modernity is conceptualized in the transformation period of first modernity to second modernity. Beck *et al* explain this as: "*reflexive modernization refers to is a distinct second phase: the modernization of modern society. When modernization reaches a certain stage it radicalizes itself. It begins to transform, for a second time, not only the key institutions but also the very principles of society. But this time, the principles and institutions being transformed are those of modern society.*"[323] Williams also stresses that "*reflexive modernity is dubbed 'reflexive' because it is an era when society begins to confront primarily itself rather than external others*"[324] It is understood that modernity criticizes itself in order to find new alternative ways to transform itself into new, real modernity. NATO's 1991 Strategic Concept is a good example of reflexive modernity, because the organisation examined itself in order to re-develop its identity in the world. Rasmussen explains this as: "*the organisation is actively reconstructing the terms of its own existence. One of Beck's central ideas is that constructivism is not only a philosophy of science but a characteristic of our times: NATO is clearly in a time of construction. In that sense, it lives up to the characteristics of reflexive modernity. An important part of reflexivity is the self-awareness brought about by reflection on one's ability to construct one's own terms of existence. NATO defines itself by the constructive character by which it has set a new security agenda.*"[325] NATO had defined the Soviet Union in Cold War term, and with the collapse of the USSR, it now has to define itself post-Cold War.

Rasmussen also uses Beck's risk society theory to identify reflexive security policies. According to him, there are three different features, being management, presence of the future and boomerang effect.[326] As stated previously, risks are not yet in existence, and Rasmussen indicates that "*risk is a scenario followed by a policy proposal for how to prevent this scenario from becoming real*".[327] But the different point of the risk in reflexive modernity is that there is no end point, because if a state has a policy to remove a risk, new risks can emerge. Rasmussen also uses Foucault's explanation of governmentality to explain

[323] Beck and *et. al*. (2003), *op.cit*., p. 1

[324] Williams (2008), *op.cit*., p. 30

[325] Rasmussen, M. V. (2001), "Reflexive Security: NATO and International Risk Society", *Millennium: Journal of International Studies*, Vol. 30 (2), p. 298

[326] *Ibid*.

[327] Rasmussen, M. V. (2006), *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century,* Cambridge: Cambridge University Press, p. 4

management. Foucault likens modern governance (governmentality) to a ship, and Rasmussen uses this term for politics guiding the ship of state to a safe harbour.[328] [329]

The importance point of the risk is the decision, and decisions can be affected by the scale and urgency of the risks. Williams explains the presence of the future as: "*The process of management becomes about managing possible events in the future-these events, which have yet to occur, become the motive for action today.*"[330] The belief is that there is a risk, which has not yet occurred, but it is the motivation of today. The main aim of the presence of the future is to obstruct these risks before they are real. Beck states that "*the center of risk consciousness lies not in the present, but in the future. In the risk society, the past loses the power to determine the present. Its place is taken by the future, thus, something non-existent, invented, fictive as the 'cause' of current experience and action*."[331] This is relevant to the reflexive point of security, because these risks may, or may not occur in the future, and important measures are taken before they occur. Williams gives an example, using the Bush administration; "*Today the gravest danger in the war on terror, the gravest danger facing America and the world, is outlaw regimes that seek and possess nuclear, chemical and biological weapons. These regimes could use such weapons for blackmail, terror, and mass murder. They could also give or sell those weapons to terrorist allies, who could use them without the least hesitation*."[332] It seems, therefore, that the United States used the presence of the future to justify its military action in Iraq.

Beck also states that if scientific technique information cannot be controlled, risk can return products to their producers. He called this the boomerang effect of risks. Beck explains the boomerang effect of risks as: "*risks of modernization sooner or later also strike those who produce or profit from them*[333]*..... Risks display a social boomerang effect in their diffusion: even the rich and powerful are not safe from them. The formerly ' latent side effects' strike back even at the centers of their production.*"[334] It can be understood that the decision on any

[328] Rasmussen (2001), *op.cit.*, p. 291

[329] Rasmussen goes on with that "risk society is open to 'rule-altering' politics because of risk's 'origin in decision-making'. In a risk society you choose the risks you take, rather than eliminate risks altogether. 'Risks are revealed as systematic events', Beck argues, 'which are accordingly in need of general political regulation'. Politics is no longer about initiating a social, economic or political process and bringing it to conclusion, that is, to the safe harbour of Foucault's metaphor. Governments no longer master ends, only means. Politics is about managing the process. In Foucault's metaphor, the rationale of government is now to keep the ship of state afloat. In these circumstances, processes become projects, as governments come to identify political success in terms of their ability to manage processes of transformation." *Ibid.*, p. 292

[330] Williams (2008), *op.cit.*, p. 62

[331] Beck (1992*), op.cit.*, p. 34

[332] Williams (2008), *op.cit.*, pp. 62-63

[333] Beck (1992), *op.cit.*, p. 23

[334] *Ibid.*, p. 37

risk can revert to the producers of the policy. Again the Iraq invasion is a good example of the boomerang effect. As stated above, the main aim of the invasion in Iraq was to obstruct the use of chemical, biological and nuclear weapons, but as Williams states, "*while the United States changed reality so that this original risk could never occur, Washington opened the flood gates that turned Iraq into the best terrorist training ground on earth. Furthermore, the United States destabilized the Middle East, which has allowed Tehran to pursue its nuclear programme without check from traditional balance Iraq.*"[335] It is clear that the first scenario lost its way, and new risks have emerged in the region. As Rasmussen infers from Beck, it can be explained as the risk trap, and any action can hold a new risk.[336]

Under the next heading, the transformation of NATO will be detailed and more information will be given about the strategic concepts of NATO and its new position in the international arena.

2.4.2. The Transformation of NATO after the Cold War

With the declaration of the London Conference in July 1990 the Cold War officially ended,[337] with a renewed focus on security, as Berdal points out:

> *"It was hardly surprising that the end of the Cold War should also have ushered in a debate about the meaning of 'international security'. The immediate instinct of many analysts and policy-makers in the West was to call for a radical redefinition of 'security studies'. The traditional focus on the role of force in international affairs, it was argued, failed to encompass the myriad of challenges and opportunities, which the post-Cold War world seemed to offer."*[338]

No one expected the end of the Cold War, including NATO. The organisation did not recognise new or developing threat perceptions, leaving the international community to question its purpose. In 1991, NATO produced a new strategic concept, and the document

[335] Williams (2008), *op.cit.*, p. 63

[336] Rasmussen (2006), *op.cit.*, p. 39

[337] The Heads of State and Government (1990), *London Declaration on a Transformed North Atlantic Alliance*, Available at: http://www.nato.int/docu/comm/49-95/c900706a.htm (Accessed at: 13/08/2012); Art, R. J. (1996), "Why Western Europe Needs the United States and NATO", *Political Science Quarterly*, Vol. 111(1), Available at: http://www.transatlantic.uj.edu.pl/upload/59_ac3f_Art.WE_Nato.pdf (Accessed at: 13/08/2012), p. 12; Aybet, G. (1999), "NATO's New Missions", *Journal of International Relations*, Vol. IV (1), Available at: http://sam.gov.tr/wp-content/uploads/2012/02/GulnurAybet3.pdf (Accessed at: 13/08/2012)

[338] Berdal, M. (1999), "International Security After the Cold War: Aspects of Continuity and Change", in Spillman, K. and Wenger, A. (1999), Towards the 21st Century: Trends in Post-Cold War International Security Policy, *Studies in Contemporary History and Security Policy*, Vol. 4, Available at: http://www.css.ethz.ch/publications/pdfs/Studien_zu_ZS-4.pdf (Accessed at: 14/08/2012), p. 23

stated that "*the monolithic, massive and potentially immediate threat which was the principal concern of the Alliance in its first forty years has disappeared. On the other hand, a great deal of uncertainty about the future and risks to the security of the Alliance remain*."[339] With the collapse of the USSR, NATO changed its conceptual shift from threat to risk, because as Elmas states, threats were known in the Cold War era and everyone had a plan to protect themselves from threat perception, but there has been uncertainty after the Cold War, and the risks can come from everywhere.[340] Rasmussen explains the new role of NATO as a rule-altering institution, and deduces that "*the organisation is actively reconstructing the terms of its own existence. One of Beck's central ideas that constructivism is not only a philosophy of science but a characteristic of our times: NATO is clearly in a time of construction. In that sense, it lives up to the characteristics of reflexive modernity. An important part of reflexivity is the self-awareness brought about by reflection on one's ability to construct one's own terms of existence. NATO defines itself by the constructive character by which it has set a new security agenda*."[341]

As stated in the Introduction, the concept of risk was seen for the first time in the 1991 NATO strategic concept of Article 7.[342] Article 8 of the strategic concept also mentions the protection of the alliance members from such risks.[343] Williams explains why NATO accepted use of the concept of risk after the Cold War: "*risk was attractive for at least two reasons. First, by highlighting the growing and increasingly random possibility of harm, it encapsulated the uncertainty of the era in a readily understandable manner. Second, risk allowed for a considerable flexibility of interpretation and so lent itself to wide variety of situations. This was important because unanimity among the allies about what specific challenges they were to address was near impossible to achieve. Risk, one sense, offered the*

[339] "The Alliance's New Strategic Concept 1991", *op.cit.*

[340] Elmas, *op.cit.*, p. 130

[341] Rasmussen (2001), *op.cit.*, p. 298

[342] NATO's 1991 Strategic Concept states that: "7.The security challenges and risks which NATO faces are different in nature from what they were in the past. The threat of a simultaneous, full-scale attack on all of NATO's European fronts has effectively been removed and thus no longer provides the focus for Allied strategy. Particularly in Central Europe, the risk of a surprise attack has been substantially reduced, and minimum Allied warning time has increased accordingly."
"The Alliance's New Strategic Concept 1991", Available at:
http://www.nato.int/cps/en/natohq/official_texts_23847.htm (Accessed at: 05/05/2016)

[343] 8.In contrast with the predominant threat of the past, the risks to Allied security that remain are multi-faceted in nature and multi-directional, which makes them hard to predict and assess. NATO must be capable of responding to such risks if stability in Europe and the security of Alliance members are to be preserved. These risks can arise in various ways." *Ibid*.

possibility of a modern interpretation of 'flexible response'."[344] A new 'security period' had begun, requiring the identification of new risks and threat perceptions, including risks posed by failed states, the development of computer and information technology, terrorism (national and international), the potential availability of biological weapons and other weapons of mass destruction, violations of human rights, poverty, people and drug trafficking, massacres and genocide, refugee problems and radicalism. These risks are mentioned in the Strategic Concept.[345] The Alliance also stated in the strategic concept that any armed attack on the territory of the Allies would be covered by Articles 5 and 6 of the Washington Treaty.[346]

Liebe accepts that the 1991 NATO strategic concept was a milestone for NATO in adapting itself to the post-Cold war era. According to him, "*NATO moved beyond the Cold War strategic framework reliant on a robust forward defense and placed new importance on the development of multinational force projection expanding the capabilities for crisis management operations and flexible deterrent options. In many respects, it provided the strategic blueprint for the military mission in the former Yugoslavia*."[347] It can be said that NATO changed its structure from identifiable threats to uncertainty, multi-faced and multi-directional risks, which are less predictable. The new 1991 strategic concept stated that these risks could be seen in different ways and would require a rapid response,[348] stressing the need for dialogue, cooperation and effective collective defence.[349]

NATO revised the 1991 strategic concept and accepted a new strategic concept in 1999. The strategic concept of 1999 reemphasised the risks, stating that

> "*the security of the Alliance remains subject to a wide variety of military and non-military risks which are multi-directional and often difficult to*

[344] Williams, M. J. (2016), "NATO and The Risk Society: Modes of Alliance Representation Since 1991", in Webber, M. and Hyde-Price, A. (2016), *Theorising NATO: New Perspectives on the Atlantic Alliance*, London: Routledge, pp. 191-192

[345] According to 1991 Strategic Concept; "Risks to Allied security are less likely to result from calculated aggression against the territory of the Allies, but rather from the adverse consequences of instabilities that may arise from the serious economic, social and political difficulties, including ethnic rivalries and territorial disputes, which are faced by many countries in central and Eastern Europe. The tensions which may result, as long as they remain limited, should not directly threaten the security and territorial integrity of members of the Alliance. They could, however, lead to crises inimical to European stability and even to armed conflicts, which could involve outside powers or spill over into NATO countries, having a direct effect on the security of the Alliance." The Heads of State and Government (1991), *The Alliance's New Strategic Concept*, Available at: http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Accessed at: 14/08/2016)

[346] *Ibid*.

[347] Liebe, L. A. (2002), NATO's New Strategic Concept: Implications for a Transforming Army, *School of Advanced Military Studies*, p. 12

[348] "The Alliance's New Strategic Concept 1991", *op.cit*.

[349] Chiarini, G. (2013), *NATO Transformation and Future Challenges*, Available at: http://www.comitatoatlantico.it/en/studi/modern-defense-and-economic-development/ (Accessed at: 10/08/2016)

> *predict. These risks include uncertainty and instability in and around the Euro-Atlantic area and the possibility of regional crises at the periphery of the Alliance, which could evolve rapidly. Some countries in and around the Euro-Atlantic area face serious economic, social and political difficulties. Ethnic and religious rivalries, territorial disputes, inadequate or failed efforts at reform, the abuse of human rights, and the dissolution of states can lead to local and even regional instability. The resulting tensions could lead to crises affecting Euro-Atlantic stability, to human suffering, and to armed conflicts. Such conflicts could affect the security of the Alliance by spilling over into neighbouring countries, including NATO countries, or in other ways, and could also affect the security of other states*."[350]

The following were identified as risks: terrorism, ethnic conflict, human rights abuses, political instability, economic fragility, and the spread of nuclear, biological and chemical weapons.[351] Significantly, these perceptions included political threats as well social and humanitarian issues, and can be seen in the cases of Iraq and Kosovo.

One of the main points of the 1999 strategic concept was to accept some fundamental tasks, enhancing security and stability in the Euro-Atlantic area; security, consultation and deterrence and defence, crisis management and partnership. The document explains these fundamental tasks as follows:

> ***"Security:*** *To provide one of the indispensable foundations for a stable Euro-Atlantic security environment, based on the growth of democratic institutions and commitment to the peaceful resolution of disputes, in which no country would be able to intimidate or coerce any other through the threat or use of force.*
>
> ***Consultation:*** *To serve, as provided for in Article 4 of the Washington Treaty, as an essential transatlantic forum for Allied consultations on any issues that affect their vital interests, including possible developments posing risks for members' security, and for appropriate co-ordination of their efforts in fields of common concern.*

[350] Heads of State and Government (1999), *The Alliance's Strategic Concept,* Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Accessed at: 19/08/2016)
[351] *Ibid*.

> ***Deterrence and Defence:*** *To deter and defend against any threat of aggression against any NATO member state as provided for in Articles 5 and 6 of the Washington Treaty.*
>
> *And in order to enhance the security and stability of the Euro-Atlantic area:*
>
> ***Crisis Management:*** *To stand ready, case-by-case and by consensus, in conformity with Article 7 of the Washington Treaty, to contribute to effective conflict prevention and to engage actively in crisis management, including crisis response operations.*
>
> ***Partnership:*** *To promote wide-ranging partnership, cooperation and dialogue with other countries in the Euro-Atlantic area, with the aim of increasing transparency, mutual confidence and the capacity for joint action with the Alliance."*[352]

Another important point of the strategic concept also reaffirmed the legality of off-site operations provided by Article 5 of the NATO Treaty,[353] thereby giving authority for NATO to conduct military operations outside its boundaries, as in Kosovo. In short, the NATO handbook explains the political elements of 1999 strategic concept as:

> *"• a broad approach to security, encompassing political, economic, social and environmental factors, as well as the Alliance's defence dimension*
>
> *• a strong commitment to transatlantic relations*
>
> *• maintenance of Alliance military capabilities to ensure the effectiveness of military operations*
>
> *• development of European capabilities within the Alliance*
>
> *• maintenance of adequate conflict prevention and crisis management structures and procedures*
>
> *• effective partnerships with non-NATO countries based on cooperation and dialogue*
>
> *• the enlargement of the Alliance and an open door policy towards potential new members*

[352] *Ibid.*

[353] *Ibid.*

• *continuing efforts towards far-reaching arms control, disarmament and non-proliferation agreements.*"[354]

These political elements of the strategic concept show that NATO has taken more responsibility to protect security and stability in the Euro-Atlantic area, the main important points of the strategic concept being crisis management, partnership, dialogue, collective defence and cooperation.[355] The extension of Article 5 of the Treaty to non-member areas could be explained in that NATO has tried to manage all crises which could create instability and insecurity in any region. Also, Wittmann states that the focus on the "Euro-Atlantic area" in the strategic concept meant to rejection of the "world policeman" role for NATO, although this area could be interpreted as "Europe and its periphery", the term periphery being an expandable term, which could take any meaning.[356]

Following the 1999 strategic concept, NATO has adapted itself during the post-Cold War era, and, as Webber states, 9/11 accelerated changes in the out of area operations of NATO.[357] Wittmann explains these significant changes in his article as: "*further significant changes were brought about by the Afghanistan war and NATO's long term engagement in support of Afghan reconstruction and state-building… by the continued and accelerating proliferation of weapons of mass destruction and missile technology; by the unfolding global terrorism and so on."*[358]

NATO has extended its operational capacity since the 9/11. The 1999 strategic concept mentioned that "*Alliance security must also take account of the global context. Alliance security interests can be affected by other risks of wider nature, including acts of terrorism, sabotage and organised crime*."[359] It is clear that NATO has accepted the risk and threat of the terrorism and this was proved by 9/11.

The concept of terrorism and the importance of 9/11 will be detailed in the next section, along with other post 9/11 threats. Other strategic concepts of NATO will be analysed in Chapter 5.

[354] NATO (2006), *Handbook*, Available at: http://www.nato.int/docu/handbook/2006/hb-en-2006.pdf (Accessed at: 17/08/2016), p. 19

[355] Wittmann, K. (2009), "Towards a New Strategic Concept for NATO", *NDC Forum Paper*

[356] *Ibid*., p. 15

[357] Webber, M. (2013), "NATO After 9/11: Theoretical Perspectives" in Hallams, E., Ratti, L. and Zyla, B. (eds) (2013), *NATO Beyond 9/11: The Transformation of the Atlantic Alliance*, Basingstoke: Palgrave Macmillan, p. 27

[358] Wittmann, *op.cit*., p. 16

[359] Heads of State and Government (1999), *op.cit.*

2.5. Emerging Threats

2.5.1. Terrorism

The concept of terrorism has become one of the most critical issues confronting the international community in terms of the threat to peace and security. It is worth noting that, over time the meaning and use of the term '*terrorism'* has changed. Since the French Revolution in 1789, concepts of terrorism have varied, but the most critical transformation occurred after 9/11. Following these attacks, terrorists began to use technological tools to threaten international peace and security. Details of why 9/11 was important for international security will be given, but before that, it is important to define the concept of terrorism. Given the significance of the threat, it is, perhaps, surprising that there is no common definition of terrorism. States[360] [361] and organisations use their own definitions. For example, some definitions of terrorism were given in the Introduction, and when these definitions are compared, each state accepts that the concept of terrorism can include threat, use of violence, obtaining of political, religious, racial or ideological objectives, and creation of fear in society. Different nations, however, have their own legal definitions which define the concept of terrorism only in their home countries, and which cannot be used in any other country. For example, Turkey has its own terrorism definition like the UK and Turkey. According to Anti-Terror Law number 3713: "*Terrorism is any kind of act done by one or more persons belonging to an organisation with the aim of changing the characteristics of the Republic as*

[360] The United Kingdom Terrorism Act 2000 interprets terrorism in the following way:
(1) In this Act "terrorism" means the use or threat of action where—
(a) the action falls within subsection (2),
(b)the use or threat is designed to influence the government [or an international governmental organisation] or to intimidate the public or a section of the public, and
(c)the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.
(2)Action falls within this subsection if it—
(a)involves serious violence against a person,
(b)involves serious damage to property,
(c)endangers a person's life, other than that of the person committing the action,
(d)creates a serious risk to the health or safety of the public or a section of the public, or
(e) is designed seriously to interfere with or seriously to disrupt an electronic system
"The Terrorism Act 2000", Available at: http://www.legislation.gov.uk/ukpga/2000/11/contents (Accessed at: 18/08/2012)

[361] Title 22 of the U.S. Code, Section 2656f (d) defines terrorism as:
(1) the term "international terrorism" means terrorism involving citizens or the territory of more than one country;
(2) the term "terrorism" means premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents; and
(3) the term "terrorist group" means any group practicing, or which has significant subgroups which practice, international terrorism.
"The title 22 of the U.S. Code", Available at: http://www.state.gov/documents/organization/65464.pdf (Accessed at: 18/08/2012)

specified in the Constitution, its political, legal, social, secular and economic system, damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish state and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat."[362] It seems clear that Turkey defines the concept of terrorism for its own security and the protection of its citizens from this threat. Mariona Llobet Angli states that the concept of terrorism "*is used indistinctly by the contending forces to criminalise their enemies and is manipulated by the different groups in a conflict to favour their own political interests. Al Qaeda or the CIA, Hamas or the Israel Defence Force, the separatists from Chechnya or Russian security forces are terrorists according to some people and freedom fighters or legitimate combatants according to others*."[363] It should be understood that all countries define the concept for their own purposes, and therefore it may not be possible to have a common understanding of terrorism in the international arena. Indeed, as Hoffman quoted from Chinlund "*one person's terrorist is another person's freedom fighter*."[364]

There have been many attempts to define the concept of terrorism in the international arena. For example, Koufa stresses that the concept of terrorism was first used in the framework of the international legal context at the Third Conference for the Unification of Penal Law in Brussels.[365] The act of terrorism was defined at the Third Conference as:

> "*[T]he intentional use of means capable of producing a common danger that represents an act of terrorism on the part of anyone making use of crimes against life, liberty or physical integrity of persons or directed against private or state property with the purpose of expressing or executing political or social ideas will be punished.*"[366]

[362] "Anti-Terror Law Number 3713", Available at: http://www.masak.gov.tr/userfiles/file/3713.pdf (Accessed at: 15/08/2016)

[363] Angli, M. L. (2013), "What does 'Terrorism' Mean?", in Masferrer, A. and Walker, C. (2013), *Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State*, Cheltenham: Edward Elgar, pp. 18-19

[364] Hoffman, P. (2004), "Human Rights and Terrorism", *Human Rights Quarterly*, Vol. 26 (4), Available at: https://muse.jhu.edu/article/174729/pdf (Accessed at: 18/07/2016), p. 936

[365] Koufa, K. (2002), "Human Rights and Terrorism in the United Nations", in Alfredsson, G. and Stravropoulou (eds.) (2002), *Justice Pending: Indigenous Peoples and Other Good Causes*, The Hague: Martinus Nijhoff Publishers, p. 205

[366] Saul, B. (2005), "Attempts to Define 'Terrorism' in International Law", *NILR*, Available at: http://www.cicte.oas.org/olat/documents/Defining%20TERRORISM%20in%20International%20Law.pdf (Accessed at: 18/07/2016), p. 59; Young, R. (2006), "Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation", *Boston College*

Although the concept of terrorism was defined for the first time in the international legal context, it did not have any legal binding on the states.

After these initiatives to define the concept of terrorism in the Conferences for the Unification of Penal Law, the League of Nations' Convention for the Prevention and Punishment of Terrorism in 1937 defined the concept of terrorism for the first time at an international level,[367] but this Convention covered only trans-national terrorism,[368] and the Convention never entered into force.[369] The Convention defined the concept of terrorism as:

> "*Criminal acts directed against a State or intended to create a state of terror in the minds of particular persons, or a group of persons or the general public.*"[370]

Although the Convention defined the act of terrorism, it was not explicit in terms of the identification of illegal acts without criminal acts.

Following the League of Nations initiatives to adopt a global definition of terrorism, the Convention on the Suppression of Financing of Terrorism was signed, and for the first time after the League of Nations attempt, sought to define the concept of terrorism.[371] According to Golder and Williams, there are two different limbs in the definition.[372] The first limb of the definition adopts a specific approach to the question by referring to certain acts[373] and the second limb to:

International and Comparative Law Review, Vol. 29 (1), Available at: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1054&context=iclr (Accessed at: 02/05/2016), p. 35; Amet, A. K. (2013), "Terrorism and International Law: Cure the Underlying Problem, Not Just the Symptom", *Annual Survey of International&Comparative Law*, Vol. 19 (1), Available at: http://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1168&context=annlsurvey (Accessed at: 18/07/2016), p. 29

[367] Human Rights Council (2010), *Counter-Terrorism and the Protection of Human Rights*, Available at: http://www.humanrightsadvocates.org/wp-content/uploads/2010/05/HRC13_Counter-terrorism_and_Human-Rights.pdf (Accessed at: 19/07/2016), p. 1; Gasser, H.P. (2002), "Acts of Terror "Terrorism" and International Humanitarian Law", *International Review of the Red Cross*, Vol. 84 (847), Available at: https://www.unodc.org/tldb/bibliography/Biblio_Int_humanitarian_law_Gasser_09_2002.pdf (Accessed at: 18/07/2016), p. 550; Young, *op.cit.*, pp. 35-36

[368] Young, *Ibid.*, pp. 35-36; Gasser, *Ibid.*

[369] Walter, C. (2004), "Defining Terrorism in National and International Law", in Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds.) (2004), *Terrorism as a Challenge for National and International Law: Security versus Liberty?*, London: Springer, p. 33

[370] Young, *op.cit..*, p. 36; Gasser, *op.cit.*, p. 552.

[371] Golder, B. and Williams, G. (2004), "What is 'Terrorism'? Problems of Legal Definition", *UNSW Law Journal*, Vol. 27 (2), Available at: http://www.tamilnation.co/terrorism/terrorism_definition.pdf (Accessed at: 28/04/2016), p. 274; Young, *Ibid.*, p. 52

[372] Golder and Williams, *Ibid.*, p. 274

[373] There are 19 universal legal instruments and additional amendments. These are; 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft; 1970 Convention for the Suppression of Unlawful Seizure of Aircraft; 1971 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation; 1973 Convention on the Prevention and Punishment of Crimes Again
st Internationally Protected Persons; 1979 International Convention against the Taking of Hostages; 1980 Convention on the Physical Protection of Nuclear Material; 1988 Convention for the Suppression of Unlawful

> "*Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in hostilities in a situation of armed conflict, when the purpose of such an act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.*"[374]

In comparison of this definition with national definitions of terrorism, it can be said that the definition requires physical violence directed at civilians,[375] but on the other hand, the object is not sufficient in national definitions.[376] Also, the definition does not mention any political, ideological or religious motivations.[377] The definition of terrorism by Convention determines the minimum requirements of terrorism, and states use their own definitions according to their national laws.

The main turning point in terrorism was the attacks on the Twin Towers on 9 September 2001. The primary significance of the 9/11 attacks was that the international community had to confront serious international terrorism.[378] Steiner *et al* explain the importance of 9/11 as "*the attacks on 11 September 2001 constituted a turning point in the relationships between international law, global institutions and terrorism*."[379] According to them, 9/11 was a turning point because, international institutions responded to the case immediately, and important resolutions passed by organisations such as the UN Security Council determined that these attacks be evaluated as a threat to international peace and security, with Resolution

Acts against the Safety of Maritime Navigation; 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf; 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection; 1997 International Convention for the Suppression of Terrorist Bombings; 1999 International Convention for the Suppression of the Financing of Terrorism; 2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf; 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; 2005 Amendments to the Convention on the Physical Protection of Nuclear Material; 2005 International Convention for the Suppression of Acts of Nuclear Terrorism; 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation; 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft; 2014 Protocol to Amend the Convention on Offences and Certain Acts Committed on Board Aircraft. "International Legal Instruments", Available at: http://www.un.org/en/counterterrorism/legal-instruments.shtml (Accessed at: 26/03/2016)

[374] "International Convention for the Suppression of the Financing of Terrorism", Available at: http://www.un.org/law/cod/finterr.htm (Accessed at: 02/05/2016)

[375] Walter, *op.cit.*, p. 13

[376] *Ibid*.

[377] *Ibid*.

[378] Gioia, A. (2006), "The UN Conventions on the Prevention and Suppression of International Terrorism, in Nesi, G. (2006) (ed.), *International Cooperation in Counter-Terrorism: The United Nations and Regional Organisations in the Fight Against Terrorism*, Aldershot: Ashgate Publishing Limited, p. 21

[379] Steiner, H. J., Alston, P. and Goodman, R. (2007), I*nternational Human Rights In Context: Law, Politics, and Morals*, Oxford: Oxford University Press, p. 380

1368 of the UN Security Council[380] which recognized the inherent right of individual or collective self-defence in accordance with the Charter.[381] This Resolution was also crucial because, for the first time, a terrorist attack had been evaluated under Article 51 of the UN Charter.[382] Steiner *et al* state that NATO and the Organisation of American States evaluated 9/11 as an armed attack and invoked the collective self-defence provisions of their treaties.[383] However, this was a different kind of threat, and it was the first time that the problem was understood as an international problem, international organisations accepting this case as an armed attack and threat to international peace and security. According to Palmer:

> *"The threat from the Irish terrorist campaign cannot be compared with the threat from Al Qaeda. The Irish campaign was domestic in nature and operated within a set of reasonably defined parameters using conventional weaponry. Those involved formed tightly knit networks. They avoided capture, had no wish to die and used warnings to restrict casualties. Eventually they were willing to engage in a political process to move forward. In contrast, Al Qaeda is global in its membership and ambition. Its networks are fluid and mobile enabling it to meet its objective of inflicting maximum loss."*[384]

The 9/11 terrorist attack was a physical, social and illegal phenomenon, which expressed itself in two distinct ways. The first is that it highlighted the personal relationship of the citizen with the threat they faced from terrorism, including the risks to public institutions and to public and private property. According to Palmer, "*after the attack any new concept of terrorism must now consider the possibility of serious harm and be sensitive to the potential social impact of a major terrorist attack. The second is the risk that terrorism presents to the values of the state that it seeks to attack*".[385] The 9/11 terrorists succeeded in their aim of creating fear and threatening policies, because the attack had both sociological and

[380] *Ibid*.; The UN Security Council (2001), *Resolution 1368*, Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement (Accessed at: 21/05/2016)

[381] *Ibid*.; Marks, S. (2006), "International Law and the 'War on Terrorism': Post 9/11 Responses by the United States and Asia Pacific Countries", *Asia Pacific Law Review*, Vol. 14 (1), Available at: https://cdn1.sph.harvard.edu/wp-content/uploads/sites/580/2012/09/spm_Terrorism_and_IL_APLR_2006_vol14.pdf (Accessed at: 21/05/2016), p. 46

[382] *Ibid*., p. 45; Quenivet, N. (2005), "The World after September 11: Has It Really Changed?", *The European Journal of International Law*, Vol. 16 (3), Available at: http://www.ejil.org/pdfs/16/3/309.pdf (Accessed at: 21/05/2016), p. 569

[383] Steiner *et al., op.cit*.; Gray, C. (2010), "The Use of Force and The International Legal Order", in Evans, M. D. (2010), *International Law*, Oxford: Oxford University Press, p. 629

[384] Palmer, P. (2011), "Dealing With the Exceptional Pre-Crime Anti-Terrorism Policy and Practice", *Policing and Society Routledge*, Vol. 22 (4), p. 11

[385] *Ibid*., p. 16

psychological impacts, which created an insecure place for citizens including military, police and public areas.[386]

After these attacks, George W. Bush announced a new strategic plan for the USA. According to the plan, pre-emptive action must be taken by countries. States could not afford to wait for terrorists to strike in their territory; collectively the international community should seek to prevent attacks.[387] The pre-emptive doctrine or Bush's doctrine provides, in a large part, the justification for the USA and its allies to attack Iraq and Afghanistan. In Iraq, the stated aim was to deal with weapons of mass destruction[388], whilst in Afghanistan, it was in order to end Taliban and Al-Qaeda actions and stop terrorist attacks in the international arena.

Following the 9/11 terrorist attacks, the United Nations Security Council adopted Resolution 1373. The importance of this resolution was the first use of Chapter VII of the UN Charter,[389] but it does not define the concept of terrorism.[390] The Convention lays significant obligation on states to fight terrorism, but the lack of at common definition of terrorism has resulted in the avoidance of fighting terrorism, or, as Young says, it masks the human rights abuses in the states.[391] In addition, Setty states that "*two serious shortcomings are immediately apparent in the framework established by Resolution 1373, though. First, although Resolution 1373 mandates that member states take serious action to counter terrorism, it lacks a definition of terrorism that would establish the parameters for the implementation of counter terrorism efforts. Second, although Resolution 1373 established the Counter-Terrorism Committee (CTC) to oversee implementation of Resolution 1373 requirements by member states, there is no textual obligation in the resolution for the CTC to safeguard human rights and the rule of law. The lack of initial focus on rights protection was only later*

[386] Perl, R. (2004), *Open For Debate: Terrorism,* New York: Benchmark Books, p.23

[387] Snauwaert, D. T. (2004), "The Bush Doctrine and Just War Theory", *The Online Journal of Peace and Conflict Resolution*, Available at: http://www.trinstitute.org/ojpcr/6_1snau.pdf (Accessed at: 20/08/2012); National Security Council (2002), *The National Security Strategy of the United States*, Available at: http://www.whitehouse.gov/nsc/nssall.html (Accessed at: 20/08/2012); See also; Cox, M. (2004), "Empire, Imperialism and the Bush Doctrine", *Review of International Studies*, Vol. 30(4), Available at: http://journals.cambridge.org/action/displayAbstract;jsessionid=E3D4DC5045BBA993ECDE33EDC796C7B0.journals?fromPage=online&aid=251273 (Accessed at: 20/08/2012), pp. 585-608. LaFeber, W. (2002), "The Bush Doctrine", *Diplomatic History*, Vol. 26 (4), Available at: http://onlinelibrary.wiley.com/doi/10.1111/1467-7709.00326/abstract (Accessed at: 20/08/2012), pp. 543-558

[388] For more information: Kull, S., Ramsay, C. and Lewis, E. (2003), "Misperceptions, The Media and the Iraq War", *Political Science Quarterly*, Vol .118(4), Available at: http://www.jstor.org/discover/10.2307/30035697?uid=3738032&uid=2&uid=4&sid=21101481037753 (Accessed at: 21/08/2012), pp. 569-598; McGoldrick, D. (2004), *From "9-11" to the "Iraq War 2003": International Law in an Age of Complexity*, Portland: Hart Publishing

[389] Young, *op.cit.*, p. 42

[390] Conte, A. (2010), *Human Rights in the Prevention and Punishment of Terrorism: Commonwealth Approaches: The United Kingdom, Canada, Australia and New Zealand,* Berlin: Springer, p. 20

[391] Young, *op.cit.*, p. 32

remedied after pressure from interests concerned with human rights. Such pressure led to passage of additional resolutions that served to remind both the CTC and member states of their obligations under the International Covenant on Civil and Political Rights as well as other protocols."[392] The CTC was established by Resolution 1373 to monitor human rights abuses, and to:

> "*Take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum seeker has not planned, facilitated or participated in the commission of terrorist acts.*"[393]

The role of CTC was limited because of the lack of definition of terrorism, but the Security Council tried to resolve this problem in 2004 with Resolution 1566.[394]

According to Resolution 1566 of the Paragraph 3;

> "*...criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature...*"[395]

According to the Human Rights Council, Resolution 1566 "*includes acts committed against civilians with both 1) the intention of causing death or serious bodily injury, or the taking of*

[392] Setty, S. (2011), "What's in a Name? How Nations Define Terrorism Ten Years After 9/11*", University of Pennsylvnia Journal of International Law*, Vol. 33 (1), Available at: https://www.law.upenn.edu/live/files/139-setty33upajintll12011pdf (Accessed at: 17/06/2016), pp. 12-13

[393] The UN Security Council (2001), *Resolution 1373*, Available at: http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/United%20Nations%20Security%20Council%20Resolution%201373%20(2001).pdf (Accessed at: 18/06/2016)

[394] Saul, B. (2015), "Terrorism in International and Transnational Criminal Law", *Legal Studies Research Paper*, No. 15 (83), Available at: http://ssrn.com/abstract=2663890 (Accessed at: 19/06/2016), p. 13

[395] Security Council (2004), *Resolution 1566*, Available at: http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1566%20(2004) (Accessed at: 18/06/2016)

hostages AND 2) for the purpose of provoking terror in the general public or in a group of persons or particular persons, intimidating a population or compelling a government or an international organisation to do or abstain from doing any act, and this Resolution will protect human rights because States will not be able to justify acts under broad or vague definitions."[396] Saul states that the definition of terrorism in Resolution 1566 is not obligatory and states cannot implicate this definition in their national laws. Rather, it "*provides guidance to state how to define the concept of terrorism is a manner which is more respectful to human rights*." [397] Although the Resolution provides guidance to states, many states had their own definitions of terrorism, and therefore the definition of terrorism by the Security Council was devised too late.

The UN General Assembly tried to define the concept of terrorism, and the Draft Comprehensive Convention on International Terrorism defines the concept of terrorism in Article 2 (1) as:

> "*Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally, causes:*
>
> *• Death or serious bodily injury to any person; or*
>
> *• Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or the environment; or*
>
> *• Damage to property, places, facilities, or systems referred to in paragraph1 (b) of this article, resulting or likely to result in major economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act*."[398]

This Convention also refers to physical violence towards any person, like the International Convention for the Suppression of Financing of Terrorism. The difference between the Draft Convention and the International Convention for the Suppression of Financing of Terrorism is that damage to property and private property is significant.[399] According to Walter, "*there seems to be a tendency in international law to extend the notion of terrorism to destructive violence against objects, which corresponds to the recent development in national legal*

[396] Human Rights Council, *op.cit*., p. 5

[397] Saul (2015), *op.cit*., p. 14

[398] "Draft Comprehensive Convention Against International Terrorism", Available at: https://www.ilsa.org/jessup/jessup08/basicmats/unterrorism.pdf (Accessed at: 19/06/2016)

[399] Young, *op.cit*., p. 55

orders."[400] Although the Draft Comprehensive Convention defines the concept of terrorism, it is still in debate, and does not have any binding status on states.[401]

Also, it must be mentioned here that there is no crime of terrorism within the jurisdiction of the International Criminal Court. Crimes of terrorism were rejected in the Draft Statute of the ICC in 1998.[402] Conte states that crimes of terrorism were rejected because the states did not have any agreement on the common definition of terrorism and it was removed from the scope of the Court.[403] Cohen explains the rejection by the states of crimes of terrorism under six headings. According to Cohen,

> "*the first and foremost obstacle to the inclusion of terrorism in the Rome Statute was the lack of a clear and universally accepted definition of what constitutes terrorism, including dissatisfaction with the proposed definition in the text of the draft. The second reason for states' reluctance to include terrorism in the Rome Statute was the notion that the three core crimes—war crimes, crimes against humanity, and genocide—represented the crimes of greatest concern to the international community, and terrorism does not rise to this level of international concern. The third ground for rejecting the inclusion of terrorism in the Rome Statute was the desire to avoid overburdening the ICC and the need for a gravity threshold. The fourth argument against the initial inclusion of terrorism in the Rome Statute was that such an inclusion would impede the acceptance of the Rome Statute. This concern is irrelevant today because the Rome Statute did, in fact, come into force and currently has 114 member states. However, similar concerns may rise with respect to the acceptance of a*

[400] Walter, op.cit., p. 36

[401] Golder and Williams, *op.cit*., p. 274

[402] Saul (2015), *op.cit*., p. 2; The Draft Statute of the ICC Article 5 defined the concept of terrorism as: "(1) Undertaking, organizing, sponsoring, ordering, facilitating, financing, encouraging or tolerating acts of violence against another State directed at persons or property and of such a nature as to create terror, fear or insecurity in the minds of public figures, groups of persons, the general public or populations, for whatever considerations and purposes of a political, philosophical, ideological, racial, ethnic, religious or such other nature that may be invoked to justify them; (2) An offence under the following Conventions: (a) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; (b) Convention for the Suppression of Unlawful Seizure of Aircraft; (c) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents; (d) International Convention against the Taking of Hostages; (e) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; (f) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf; (3) An offence involving use of firearms, weapons, explosives and dangerous substances when used as a means to perpetrate indiscriminate violence involving death or serious bodily injury to persons or groups of persons or populations or serious damage to property."

[403] Conte, *op.cit*., p. 20

> *new crime of terrorism. As will be elaborated ahead, any amendment to the Rome Statute does not apply automatically to all the states parties but rather applies only to those states parties that have ratified it specifically. A fifth argument is based on a more practical level; some states questioned the need to include terrorism in the Rome Statute because, as a treaty crime, there was already in place a system of international cooperation to deal with it. The sixth and final objection to the inclusion of the terrorism in the Rome Statute argued that since terrorism is such a politically-sensitive term, if the ICC would deal with cases of terrorism, it will be forced into the political realm and thus will hurt its legitimacy and credibility as an impartial judicial institution*."[404]

Cohen's observations may be true for the rejection of the jurisdiction of the crimes of terrorism by the ICC, but, as Cohen states, only one reason can be more effective than others, and it is the lack of a definition of the terrorism.[405] Also, the sixth reason can affect the role of the ICC in the jurisdiction, because as mentioned above that "*one person's terrorist is another person's freedom fighter",*[406] and this is also related to the lack of a common definition of terrorism. Although the international community has established many mechanisms to fight terrorism, the lack of definition has affected the role of these mechanisms. The ICC Statute may only prosecute terrorist acts if they reach the threshold of war crimes, crimes against humanity, or genocide.[407]

On the other hand, international humanitarian law prohibits any form of terrorism committed as international or non-international armed conflict,[408] "*including deliberate attacks on civilians or civilian objects, indiscriminate attacks, reprisals, the use of prohibited weapons, attacks on cultural property, objects indispensable to civilian survival, or works containing*

[404] Cohen, A. (2012), "Prosecuting Terrorists at the International Criminal Court: Reevaluating an Unused Legal Tool to Combat Terrorism", *Michigan State International Law Review*, Vol. 20 (2), Available at: http://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1080&context=ilr (Accessed at: 20/06/2016), pp. 224-228

[405] *Ibid*., p. 229.

[406] Footnote 360

[407] UNODC (2009), *International Law Aspects of Countering Terrorism*, Available at: https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf (Accessed at: 21/06/2016), p. 40

[408] Condorelli, L. and Naqvi, Y. (2004), "The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of Date?", in Bianchi, A. (ed.) (2004), *Enforcing International Law Norms Against Terrorism*, Oxford: Hart Publishing, p. 30; Gasser, H. P. (1986), "Prohibition of terrorist Acts in International Humanitarian Law", *International Review of the Red Cross*, Vol. 26 (253), p. 212; Weatherall, T. (2015), "The Status of the Prohibition of Terrorism in International Law: Recent Developments", *Georgetown Journal of International Law*, Vol. 46, Available at: https://www.law.georgetown.edu/academics/law-journals/gjil/recent/upload/zsx00215000589.PDF (Accessed at: 20/07/2016); Gasser (2002), *op.cit*., p. 549; Saul (2015), *op.cit*., p. 4

dangerous forces (including dams, dykes and nuclear facilities); or through illegal detention, torture or inhuman treatment."[409] Gasser explains the international humanitarian law approach for in two different reasons. According to him; "*First, the right to use force and commit acts of violence is restricted to the armed forces of each party to an armed conflict. Only members of such armed forces have the "privilege" to use force against other armed forces, but their right to choose methods or means of warfare is not unlimited. On the other hand, only members of armed forces and military objectives may be the target of acts of violence. Second, other categories of persons, in particular the civilian population, or of objects, primarily the civilian infrastructure, are not legitimate targets for military attacks — they are, in the words of the Geneva Conventions, "protected" and must in all circumstances be spared*."[410] It is clear that international humanitarian law prohibits attacks on civilians during armed conflict, and that if any part of the armed conflict targets the civilian population, the states will be punished. Also Article 33 of the IV Geneva Convention in 1949 states that:

> "*No protected person may be punished for an offence he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited.*
>
> *Pillage is prohibited.*
>
> *Reprisals against protected persons and their property are prohibited*."[411]

Saul mentions that Article 33 of the IV Geneva Convention was a response to the mass intimidation of civilians in the Second World War.[412] Also Protocol 1 Additional to the Geneva Conventions in 1977 protects civilians in international conflict. According to Article 51 (2) of the Protocol 1:

> "*The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.*"[413]

Additional Protocol 1 also stresses the protection of civilians during armed conflicts, and prohibits the threats of violence against the civilian population. With this Protocol 1, the IV Geneva Convention is expanded in terms of intention. The meaning of the Article is, briefly,

[409] Saul (2015), *Ibid*.

[410] Gasser (2002), *op.cit.*, p. 554

[411] "Convention IV Relative to the Protection of Civilian Persons in Time of War", Available at: https://ihl-databases.icrc.org/ihl/385ec082b509e76c41256739003e636d/6756482d86146898c125641e004aa3c5 (Accessed at: 21/06/2016)

[412] Saul (2015), *op.cit.*, p. 4

[413] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1)", Available at: https://ihl-databases.icrc.org/ihl/WebART/470-750065 (Accessed at: 21/06/2016)

that intention is the one of the important elements of the definition of acts of terrorism.[414] Protocol 2 also prohibits acts of terror in non-international conflicts.[415]

According to Saul, "*the International Criminal Tribunal for the former Yugoslavia (ICTY) was the first international tribunal to recognise 'the crime of terror as a violation of the laws or customs of war' in the Tadic*[416] *case"*.[417] It seems clear that international humanitarian law strongly prohibits terror among civilian persons, and the first prosecution was seen in the ICTY. As was stated above, the ICC prosecutes terrorist acts if they threshold to war crimes, crimes against humanity, or genocide and the case of Tadic shows us that terrorist acts can be considered as war crimes.[418]

Although the Conventions and Protocols prohibit acts of terror, there is no definition of terror in these documents, and the ICTY, likewise did not define the concept. The Appeal Chamber of the Special Tribunal for Lebanon (STL) found a definition of terrorism under the customary international law.[419] The Appeal Chamber of the STL used the definition of terrorism by the International Convention for the Suppression of the Financing of Terrorism. According to Cohen, the Appeal Chamber was right and the Convention's definition of terrorism can be accepted as a *de facto* internationally acceptable definition.[420]

[414] Gasser (2002), *op.cit.*, p. 556

[415] Article 4 of the Protocol 2 states that: "Article 4 [Link] -- Fundamental guarantees
1. All persons who do not take a direct part or who have ceased to take part in hostilities, whether or not their liberty has been restricted, are entitled to respect for their person, honour and convictions and religious practices. They shall in all circumstances be treated humanely, without any adverse distinction. It is prohibited to order that there shall be no survivors.
2. Without prejudice to the generality of the foregoing, the following acts against the persons referred to in paragraph 1 are and shall remain prohibited at any time and in any place whatsoever:
(a) violence to the life, health and physical or mental well-being of persons, in particular murder as well as cruel treatment such as torture, mutilation or any form of corporal punishment;
(b) collective punishments;
(c) taking of hostages;
(d) acts of terrorism;
(e) outrages upon personal dignity, in particular humiliating and degrading treatment, rape, enforced prostitution and any form of indecent assault;
(f) slavery and the slave trade in all their forms;
(g) pillage;
(h) threats to commit any of the foregoing acts."
Article 13 (2) of the Protocol 2 states that: "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."
"Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol 2)", Available at: https://ihl-databases.icrc.org/ihl/INTRO/475?OpenDocument (Accessed at: 21/06/2016)

[416] This case is not the scope of the research. Therefore the detail of the case is not given.

[417] Saul (2015), *op.cit.*, pp. 4-5

[418] Cohen, *op.cit.*, p. 247-248

[419] *Ibid.*, p. 230

[420] *Ibid.*, p. 231

The above information shows us that the lack of definition of the concept of terrorism has created many problems in the international area in terms of the cooperation between states, human rights and information exchange. This situation also blocked the jurisdiction of the ICC on the terrorism issue and the crimes of terrorism were rejected by the states.

For the purposes of this paper, I intend to adopt the following definition of the concept of terrorism:

> *"(1) In this Act "terrorism" means the use or threat of action where—*
> *(a) the action falls within subsection (2),*
> *(b)the use or threat is designed to influence the government [or an international governmental organisation] or to intimidate the public or a section of the public, and*
> *(c)the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.*
> *(2)Action falls within this subsection if it—*
> *(a)involves serious violence against a person,*
> *(b)involves serious damage to property,*
> *(c)endangers a person's life, other than that of the person committing the action,*
> *(d)creates a serious risk to the health or safety of the public or a section of the public, or (e) is designed seriously to interfere with or seriously to disrupt an electronic system."*[421]

There were a number of reasons for choosing this definition. Firstly, as stated above, the Additional Protocol 1 of the IV Geneva Conventions covers one of the main elements of the definition, which is 'intention'. Moreover, the UK's definition of terrorism also includes the intention of terrorists in all cases. Secondly, this definition covers the above mentioned definitions in terms of damage to property and political, ideological, or religious purposes. Thirdly, the definition uses the concept of risk in terms of public health and safety. Lastly, as Walter states, the UK Terrorism Act 2000 covers threat or damage to computer installations (disruption of electronic systems). [422] The last reason explains the importance of the future in terms of taking measures against the risks and threats. In recent years, the international community has faced different problems, such as cybercrime and cyber terrorism, but no legal or scholarly definitions have appeared to cover this risk in their definition of terrorism.

[421] "The Terrorism Act 2000", op.cit.

[422] Walter, *op.cit.*

The above definition was chosen because it covers all aspects of terrorism, and can be used by states, or accepted as an international definition of terrorism.

Coming back to pre-emptive doctrine (Bush doctrine), it has failed to prevent terrorism in the international arena. According to Elmas, pre-emptive strategies or doctrines are risk scenarios, and are based on the worst events which could occur in the future to affect the world in terms of security and peace.[423] Pre-emptive doctrines are not based on evidences, but on suspicions.[424] Beck explains this situation as a real '*virtuality'* and he quotes the example of the Second Iraq War as, "*conducted in order to prevent what we cannot know, that is, whether and to what extent chemical and nuclear weapons of mass destruction get into the hands of terrorists*."[425] As stated previously, the invasion of Iraq was to obstruct the use of chemical, biological and nuclear weapons, and, as Williams infers, "*while the United States changed reality so that this original risk could never occur, Washington opened the flood gates that turned Iraq into the best terrorist training ground on earth. Furthermore, the United States destabilized the Middle East, which has allowed Tehran to pursue its nuclear programme without check from traditional balance Iraq*"[426]. This scenario lost its position and new risks have emerged in the region. As Heng suggests there was no Al Qaeda presence before the war, but in aftermath of the war, the region attracted terrorists from around the world.[427] Therefore, this policy has failed to prevent terrorist attacks. For example some terrorist attacks occurred after the war such as: in November 2003, bomb attacks were carried out in Istanbul in the buildings of HSBC, the British Consulate, and the Beth Israel and Neve Shalom Synagogues.[428] On 11 March 2004, terrorists bombed trains in Madrid, Spain.[429] Al-

[423] Elmas, *op.cit*., p. 173
[424] *Ibid*., p. 174
[425] Beck, U. (2006), "Living in the World Risk Society", *Economy and Society,* Vol. 35 (3), Available at: http://www.skidmore.edu/~rscarce/Soc-Th-Env/Env%20Theory%20PDFs/Beck--WorldRisk.pdf (Accessed at: 22/06/2016), p. 335
[426] Williams (2008), *op.cit*., p. 63
[427] Heng, Y. K. (2006), "The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society", *International Relations,* Vol. 20 (1), Available at: http://ire.sagepub.com/content/20/1/69.full.pdf+html?hwshib2=authn%3A1472486035%3A20160828%253Aac9c830f-b0c0-4084-9f42-11b0f3c242a4%3A0%3A0%3A0%3AePN6ZQXBeRR1k%2FrdPv5wMA%3D%3D (Accessed at: 23/06/2016), pp. 85-86
[428] For more information: "Istanbul Rocked by Double Bombing", Available at: http://news.bbc.co.uk/1/hi/world/europe/3222608.stm (Accessed at: 21/08/2012). "The Softest Target", Available at: http://www.guardian.co.uk/world/2003/nov/23/turkey.terrorism (Accessed at: 21/08/2012) "Istanbul Truck-Bomb Attacks Kill 27", Available at: http://www.foxnews.com/story/0,2933,103612,00.html (Accessed at: 21/08/2012). "Bomb Wounds 8 in Heart of Istanbul", Available at: http://www.nytimes.com/2011/05/27/world/europe/27turkey.html?_r=0 (Accessed at: 21/08/2012)
[429] For more information**:** Reinares, F. (2012), *The Evidence of Al-Qa'ida's Role in the 2004 Madrid Attack,* Available at: http://www.ctc.usma.edu/posts/the-evidence-of-al-qaidas-role-in-the-2004-madrid-attack (Accessed at: 21/08/2012). "The 2004 Madrid Bombings", Available at: http://www.guardian.co.uk/world/2007/oct/31/spain.menezes (Accessed at: 21/0/2012). "Terrorist Bomb Trains

Qaeda attacked London in 2005, when the public transport system was bombed during rush hour.[430] The last terrorist attack in Europe by ISIS was in Istanbul in 2016.[431]

Although there have been many international agreements, terrorist organisations continue to use violence and technology to achieve their aims.[432] These attacks show us that terrorist organisations can attack at any moment and anywhere in the world coupled with the believe that terrorist groups might acquire biological and nuclear weapons it almost goes without saying that terrorism is now the most influential threat to the international community.

The significance of the 9/11attacks for this thesis is that for the first time the Allies sought to invoke Article 5 of the NATO Treaty.[433]

in Madrid", Available at: http://www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid (Accessed at: 21/08/2012)

[430] For more information: "2005: Bomb Attacks on London", Available at: http://news.bbc.co.uk/onthisday/hi/dates/stories/july/7/newsid_4942000/4942238.stm (Accessed at: 21/08/2012). "Report of the Official Account of the Bombings in London on 7th July 2005", Available at: http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf (Accessed at: 21/08/2012). "7 July 2005 London Bombings", Available at: http://www.martinfrost.ws/htmlfiles/london_bombs2.html (Accessed at: 21/08/2012)

[431] For more information: "Istanbul Airport Attack: Turkey Blames ISIS as New Details Merge of Assault", Available at: https://www.theguardian.com/world/2016/jun/29/istanbul-ataturk-airport-attack-turkey-declares-day-of-mourning (Accessed at: 07/07/2016); "Istanbul Terror Attack: Erdogan Says Turkey Will not be Divided", Available at: http://edition.cnn.com/2016/06/29/europe/turkey-istanbul-ataturk-airport-attack/ (Accessed at: 07/07/2016); "ISIS Leadership Involved in Istabul Attack Planning, Turkish Source Says", Available at: http://edition.cnn.com/2016/06/30/europe/turkey-istanbul-ataturk-airport-attack/ (Accessed at: 07/07/2016)

[432] There are 19 universal legal instruments and additional amendments. These are; 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft; 1970 Convention for the Suppression of Unlawful Seizure of Aircraft; 1971 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation; 1973 Convention on the Prevention and Punishment of Crimes Again
st Internationally Protected Persons; 1979 International Convention against the Taking of Hostages; 1980 Convention on the Physical Protection of Nuclear Material; 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf; 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection; 1997 International Convention for the Suppression of Terrorist Bombings; 1999 International Convention for the Suppression of the Financing of Terrorism; 2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf; 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; 2005 Amendments to the Convention on the Physical Protection of Nuclear Material; 2005 International Convention for the Suppression of Acts of Nuclear Terrorism; 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation; 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft; 2014 Protocol to Amend the Convention on Offences and Certain Acts Committed on Board Aircraft. "International Legal Instruments", Available at: http://www.un.org/en/counterterrorism/legal-instruments.shtml (Accessed at: 26/03/2016)

[433] "NATO Summit Guide", Available at: http://www.nato.int/lisbon2010/summit-guide-eng.pdf (Accessed at: 23/08/2012)

2.5.2. Cybercrime

In this section I will aim to define the concept of cybercrime, before further explaining and analysing the main concept discussed in this thesis, cyber terrorism.

Cybercrime is a relatively new phenomenon. Since the invention of the PC and the Internet, the international community has had to tackle this threat. Cybercrime is also referred to as "computer crime," "information crime," and "internet crime".

As there is no common definition of the concept of cybercrime,[434] it may be helpful to explain the terms "cyber" and "crime" individually. The American Heritage Dictionary of Student Science defines the term "cyber" as: "*A prefix that means 'computer' or 'computer network,' as in cyberspace, the electronic medium in which online communication takes place*."[435] The Oxford Dictionary explains it by stating that it "*[r]elat[es] to or [is] characteristic of the culture of computers, information technology, and virtual reality.*"[436] Lastly, Finland explains the concept as follows:

> *"The word 'cyber' is almost invariably the prefix for a term or the modifier of a compound word, rather than a stand-alone word. Its inference usually relates to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems. Only the complete term of the compound word (modifier+head) itself can be considered to possess actual meaning. The word cyber is generally believed to originate from the Ancient Greek verb, κυβερεω (kybere) 'to steer, to guide, to control'."*[437]

The concept "crime" is explained by the Oxford Dictionary as "*[a]n action or omission which constitutes an offence and is punishable by law*"[438]; Merriam-Webster, on the other hand, explains it as follows: "*an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law*."[439]

[434] O'Brien, M., *Computer Crime*, Available at: http://www.mobrien.com/computer_crime1.htm (Accessed at: 01/02/2015)

[435] "The Meaning of Cyber", Available at: http://www.thefreedictionary.com/cyber- (Accessed at: 01/02/2015)

[436] "Cyber", Available at: http://www.oxforddictionaries.com/definition/english/cyber (Accessed at: 01/02/2015)

[437] Government Resolution (2013), *Finland's Cyber Security Strategy*, Available at: http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf (Accessed at: 20/02/2015), p. 12

[438] "Crime", Available at: http://www.oxforddictionaries.com/definition/english/crime (Accessed at: 01/02/2015)

[439] "Crime", Available at: http://www.merriam-webster.com/dictionary/crime (Accessed at: 01/02/2015)

By combining these definitions, cybercrime can simply be explained as a crime or illegal action committed by using information technologies or a computer. The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders which was held in Vienna in 2000 defines cybercrime as "*…refer[ring] to any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment."*[440] Whatever the defining features of cybercrime is that it is an illegal action conducted by using information technology or the Internet.

Nevertheless, there are many controversies surrounding the definitions of cybercrime. For instance, the concept has been both narrowly and broadly defined. The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders held in Vienna in 2000 divided the concept into two sub-categories. They are listed as follows:

> *a) Cybercrime in a narrow sense ("computer crime"): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;*
>
> *b) Cybercrime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*[441]

Furthermore, the Department of Justice (DOJ), the USA defines this concept broadly as "*any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution*."[442] Forester and Morrison also define the concept of computer crimes more narrowly in their book: viz., as "*a criminal act that has been committed using a computer as the principal tool*."[443]

I suggest that such crimes must include an element either of self-interest or group-interest, and must be aimed at destroying things. Ergo, cybercrime can be explained as: *[a]n illegal action [being] directed or committed at [a] computer or information technology to destroy [something] or create… fear [within] society for self* - *or group-interest.*

[440] United Nations (2010), *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna*, Available at: http://www.uncjin.org/Documents/congr10/10e.pdf (Accessed at: 01/02/2015), p.4

[441] *Ibid.*

[442] Parker, D. B. (1989), *Computer Crime: Criminal Justice Resource Manual*, Available at: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf (Accessed at: 02/02/2015), p.2

[443] Forester, T. and Morrison, P. (2001), *Computer Ethics*, MIT: MIT Press, p. 29

As with the definition of cybercrime, there are many differences in the typologies and classifications of cybercrime. Some of these will now be presented. For instance, the Convention on Cybercrime recognises four different types of cybercrime offences. These include:

1) *offences against confidentiality;*
2) *the integrity and availability of computer data and systems;*
3) *computer-related offences and content-related offences; and*
4) *copyright-related offences.*[444]

Moreover, Carter classifies cybercrime into four different categories. They are listed as follows:

1) *Computer as the Target: these types of cybercrime include the theft of marketing information, such as the name and information of people, the sabotage of intellectual property or personnel data, or the sabotage of operating systems and programs.*
2) *Computer as the Instrumentality of the Crime: this type of cybercrime mainly includes fraud cases. For instance, credit card fraud and telecommunications fraud. With regard to these two types of cybercrime, the computer is essential for committing the crime.*
3) *Computer is Incidental to other Crimes: Like the other two types of cybercrime, the computer is not the essential tool for committing the cybercrime. The crime will occur without the use information technologies. Money laundering, child pornography and unlawful banking transfers can be examples of this kind of cybercrime.*
4) *Crimes associated with the Prevalence of Computers: this type of cybercrime includes copyright violations of computer programs or software, as well as the theft of technological equipment.*[445]

Even though scholars and international organisations have classified cybercrime into different categories, the Convention on Cybercrime[446]is the only clear international agreement which seeks to prevent these types of crimes from being committed in the international arena.

[444] "Convention on Cybercrime", Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Accessed at: 02/02/2015)

[445] Carter, D. L. (1995), *Computer Crime: How Techno-Criminals Operate*, Available at: http://www.lectlaw.com/files/cri14.htm (Accessed at: 02/02/2015)

[446] "Convention on Cybercrime", *op.cit.*

Unfortunately only 49 countries have signed and ratified the Convention.[447] Although 49 countries signed and ratified it, there have been many reservations concerning the Convention, and these reservations have hampered the harmonization of the Convention with existing domestic law. Weber states that "*the Convention represents only an illusory attempt to harmonize cybercrime laws between its prospective members. The reservations permit parties to preserve their existing laws and undermine harmonization. As a result of these reservations, it is unclear which parties, if any, will need to adjust their current domestic law to be in compliance with the treaty*."[448] It can be understood from the reservations that universal cooperation is blocked on cybercrime legislation. Another problem with the Convention on Cybercrime is that when the states signed the Convention, the ratification took too much time, after which, if there was no reservation, states tries to adapt it to their domestic law.[449] For example, Turkey signed the Convention in 2010, but only ratified it in 2014, and it came into force in 2015; likewise, the United Kingdom signed the Convention in 2001, but only ratified it in 2011.[450] Moreover, Marion argues that states may ratify the Convention, but this is not to say that these states will implement the laws, because there is no international policing to enforce the provisions,[451] "*since the treaty is not legally binding on the states and harmonizing measures will have only limited effect. Although such cooperation between governments sounds effective in theory, it is very difficult to achieve in practice*."[452] It seems clear that the signature of the Convention is not important, but that the ratification and the implementation of the Convention are more important than the signature. Moreover, there are different problems with the Convention on Cybercrime. Marion identifies these problems as, "*Although the treaty tried to define terms and create some sort of consistency, critics of the treaty say that its provisions lack clarity and are unclear and provide only very vague definitions of some of the terms. For example, the definition of 'Illegal Devices' lacks sufficient specificity to ensure that it will not become an all-purpose basis to investigate individuals engaged in computer-related activity that is completely lawful.*

[447] "Council of Europe Treaty Office", Available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (Accessed at: 02/02/2015)

[448] Weber, A. M. (2003), "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal*, Vol. 18 (1), Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj (Accessed at: 25/05/2016), pp. 443-444

[449] *Ibid*.

[450] "Council of Europe Treaty Office", *op.cit.*

[451] Marion, N. E. (2010), "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation", *International Journal of Cyber Criminology*, Vol. 4 (1&2), Available at: http://www.cybercrimejournal.com/marion2010ijcc.pdf (Accessed at: 25/05/2016), p. 703

[452] *Ibid*.

As another example, the term 'service provider' is defined in the treaty as any public or private entity that provides a service via the computer or any entity that stores data for such an online service. Critics say that under this definition, a pizza delivery operation could be considered a service provider. Because the terms are so broad, the treaty will be difficult to enforce."[453] Also, it must be mentioned here that lack of a common definition of threats or concepts creates these problems in the universal agreements. Each country or state has their own definition of threats such as terrorism and cybercrime, because they may have different and very difficult problems in their territories, and this can affect the definitions and interpretations of the concepts.

As stated above, the Convention on Cybercrime is an international agreement on cybercrime issues, but only 49 have countries signed and ratified it. Schell and Martin mention that "*the signatory countries are not the 'problem countries'.*[454] *Crackers frequently route attacks through portals in Yemen or North Korea, where no comparable legislation exists and where cybercriminals are relatively safe from prosecution*." Lagazio additionally states that "*these countries, Yemen and North Korea, most need to sign the Convention in order for it to be effective*."[455] To evaluate all the information concerning the Convention on Cybercrime, it may be said that if problematic states like Yemen and North Korea do not sign it, and states cannot ratify or implement the laws of the Convention in their domestic law, the Convention on Cybercrime will lose its importance in the international arena. Also, Marion states that the Convention on Cybercrime is largely symbolic, because it has many problems relating to the definitions of terms and privacy issues and it is difficult to enforce states into cooperation because of the lack of international police.[456]

In short, the Convention on Cybercrime has many problems and if these problems cannot solved, the efficiency of the Convention can lose its position in the near future and if many states sign, including problem states, ratify and implement the laws of the Convention without reservations, the Convention can be accepted as a universal agreement. Above problems show us that why a few countries signed and ratified the agreement, and we learn from the Convention on cybercrime that if writers or drafters of the international agreements

[453] *Ibid*., p. 705

[454] Schell, B. H. and Martin, C. (2004), *Cybercrime: A Reference Handbook,* California: ABC-CLIO, p. 103

[455] Lagazio, M. (2016), "A Taxonomy of Cybercrime in the Financial Sector: A Comprehensive Approach to Countermeasures", in Taplin, R. (2016), *Managing Cyber Risk in the Financial Sector: Lessons From Asia, Europe and the USA*, New York: Routledge, p. 56; Archick, K. (2006), "Cybercrime: The Council of Europe Convention", *CRS Report for Congress,* Available at: http://www.au.af.mil/au/awc/awcgate/crs/rs21208.pdf (Accessed at: 25/05/2016), p. 3

[456] Marion, *op.cit*., p. 709

cannot care states interests, their special problems and do not define the terms in clear form, the agreement can lose its international agreement position and can have many criticism on it.

2.5.4. Cyber Terrorism

After the Cold War, there were also many developments in information technology, including data transfer, faster communication and the possibility of cultural interactions between different people. This development has created new threat perceptions for states, because they are unable to obstruct information transfer and other tools associated with computer technology. There have been many cyber-attacks against states and organisations, for instance in Estonia, Georgia and on NATO.

With the developments in technology and information technology, cyberspace has become a tool for terrorists to attack states and international organisations (e.g. information warfare and cybercrime). The attack on Estonia, which lasted for more than three weeks, suggests that the resulting negative consequences could damage people’s lives, impact on communities and businesses and adversely affect government prestige.

Although I gave some definitions in the introduction of the thesis, some other definitional issues below, I would characterise cyber terrorists as individuals who coerce or intimidate an organisation or government by launching cyber-attacks against a network or individual computers - including the information stored on them - for the purpose of advancing their own social or political aims, targets, or objectives. They use computer resources, networks, the Internet, etc., in order to undertake real attacks. These may include hacking activities which are directed towards families and ordinary people in general, organised through groups within networks that attempt to collect information in order to ruin individual lives. These kinds of threats include blackmail, robberies, etc.

There are various types of terrorists involved in cybercrimes, such as groups of professional crackers/hackers, whose work is solely motivated by money. These types of hacker often hack a competitor’s site for the purpose of accessing valuable, reliable and credible information.

Organised terrorist hackers, on the other hand, often wish to accomplish a specific goal. These goals are usually affected by a particular political bias, e.g. fundamentalism. Some nations use such terrorists to hack the government information of the opposing nation for political gains, or in order to block that nation's political or social decisions,[457] as was the case for Estonia in 2007.

The new face of terrorism is dangerous because it does not have any limits, due to its use of cyberspace. Also, there is no need for any of the usual bloody actions that terrorists have used historically (e.g. bombing, kidnapping and weapons). According to Hawks, "*[t]hey can send viruses to computer systems [of] critical importance and paralyze the military, political and economic resources of one country, or even a continent*."[458]

Furthermore, I would suggest that cyber terrorism is more effective than other types of terrorism, not simply because it is cheaper, but also because it is almost impossible for states and international organisations to track the cyber terrorists. According to Weimann, "*[c]yber terrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organisations to recruit and retain followers*."[459] Moreover, attackers have more options than their counter-terrorism counterparts. Weimann explains this as follows: "*The cyber terrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit*."[460] There is therefore an obvious danger of attacks on both governmental and public utilities, creating fear, which could achieve more success than other types of terrorism.

As with the concept of terrorism and cybercrime, there is no common definition of cyber terrorism. Rather, there are numerous definitions. For example, Denning explains the concept as follows:

> *"Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to*

[457] Hardy, K. and Williams, G. (2014), "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism", in Chen, T. M., Jarvis, L. and Macdonald, S. (eds.) (2014), *Cyberterrorism: Understanding, Assessment, and Response*, London: Springer, p. 2

[458] Hawks, B. B. (2011), *Cyber Terror: The Borderless Danger*, Available at: http://www.inter-disciplinary.net/wp-content/uploads/2011/05/banuhawksepaper.pdf (Accessed at: 11/04/2012), p. 1

[459] Weimann, G. (2004), "Cyberterrorism: How Real Is the Threat?", *United States Institute of Peace Special Report No.119*, Available at: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=14122&lng=en (Accessed at: 10/03/2015), p. 6

[460] *Ibid.*

> *generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not."*[461]

Denning's definition also includes non-violent actions such as cyber terrorism, given the appropriate circumstances (viz. when she says that they should "*at least cause enough harm to generate fear*").[462] Taliharm states that Denning's interpretation of cyber terrorism "*creates a distinction between a cyber-terrorist and a malicious hacker, prankster, identity thief, cyber-bully, or corporate spy based on the political motivation of the attacker. It also differs from hacking, cracking, phishing, spamming, and other forms of computer-related abuse, though cyber terrorists may use these tactics".*[463] Denning's explanation of cyber terrorism is narrow because as Jarvis *et al* state, "*the main target of an attack differentiate this type of politically motivated activity from others*."[464] In short, the definition does not require that an attack be committed via a computer, but the main targets of the attack are computers or networks.[465]

Another explanation was provided by the Centre for Strategic and International Studies (CSIS) in 1998, suggesting that:

> *"Cyber terrorism means premeditated, politically motivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets*."[466]

[461] Denning, D. E. (2003), *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, H. Comm. on the Armed Services*, Available at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Accessed at: 07/11/2013); See also; Conway, M. (2004), *Cyberterrorism: Media Myth or Clear and Present Danger?*, Available at: http://doras.dcu.ie/505/1/media_myth_2004.pdf (Accessed at: 29/02/2012), pp.3-4

[462] Denning, D. (2000), *Cyberterrorism*, Available at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Accessed at: 02/03/2012)

[463] Taliharm, A. M. (2010), "Cyberterrorism: in Theory or in Practice?", *Defence Against Terrorism Review*, Vol. 3 (2), p. 65

[464] Jarvis, L., Nouri, L. and Whiting, A. (2014), "Understanding, Locating and Constructing Cyberterrorism", in Chen, T. M., Jarvis, L. and Macdonald, S. (eds.) (2014), *Cyberterrorism: Understanding, Assessment, and Response*, London: Springer, p. 28

[465] Bishop, P. (2015), "Cyberterrorism, Criminal Law and Punishment-Based Deterrence", in Jarvis, L., Macdonald, S. and Chen, T. M. (eds.) (2015), *Terrorism Online: Politics, Law and Technology*, Oxon: Routledge, p. 109; Macdonald, S. and Jarvis, L. (2014), "What is Cyberterrorism? Findings From a Survey of Researchers", *Terrorism and Political Violence*, Vol. 27 (4), Available at: http://www.tandfonline.com/doi/full/10.1080/09546553.2013.847827 (Accessed at: 22/07/2016), p. 660

[466] Colarik, A. (2006), *Cyber Terrorism Political and Economic Implications*, London: Idea Group Publishing, p. 46

This definition is also narrow because it does not require any attack to be perpetrated via a computer, and only politically motivated attacks can be accepted as cyber-terrorist attack.

Moreover, Lewis defines the concept in an even narrower way: "*the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.*"[467] Lewis' definition is not only narrow, but also does not mention the level of coercion and intimidation required in order to define an attack as being a cyber-terrorist attack, or how cyber terrorists shut down critical national infrastructures. Therefore, it is not possible to accept this definition as a description of cyber terrorism.

In the legal context, Hardy and Williams claim that cyber-attacks can be evaluated under the Terrorism Act 2000 of the United Kingdom. According to them, the definition of terrorism includes intention requirement, motive requirement, or harm requirement, and, according to Article 2(e) of the Act, "*designed seriously to interfere with or seriously to disrupt an electronic system*". Another important factor is that the Terrorism Act starts with the '*use or threat of action where…*', which means that a person who threatens to perpetrate a terrorist act would fall under the definition.[468] They continue to explain how the Terrorism Act 2000 is useful in identifying cyber-attacks as: "*Firstly, it is clear that the definition would apply to the threat of a cyber-attack in the same way that it would apply to an actual cyber-attack. Secondly, the definition would apply to cyber-attacks that are designed merely to 'influence' a government. No higher standard of intention—such as 'coercing' or 'intimidating' a government—is required. Thirdly, the definition would apply to cyber-attacks against 'international governmental organisations' such as the United Nations or NATO. Fourthly, to qualify as an act of terrorism, a cyber-attack need not seriously interfere with critical infrastructure such as a power grid or nuclear power station; the attack could seriously interfere with anything that the courts consider to be an 'electronic system'. This could plausibly include website servers affected by a flood of emails under a DDoS attack launched by a hacktivist group. Indeed, the fact that sub-section (2)(e) uses the phrase ' designed to ' suggests that a cyber-attack would not need to actually cause any interference; the mere intention of causing interference would be enough for an individual to be prosecuted for terrorism. Fifthly, the definition would apply to cyber-attacks designed to influence oppressive foreign regimes. Lastly, there is no specific exemption for cyber-attacks that could*

[467] Lewis, J. A. (2002), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", *CSIS*, Available at: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (Accessed at: 11/03/2015), p.1

[468] Hardy and Williams, *op.cit*., p. 5

be classified as political protest or self-determination."[469] This explanation shows that cyber-terrorists or individuals will be prosecuted under the Terrorism Act 2000.[470]

Additionally, Fidler states that the Special Tribunal for Lebanon explains the international crime of terrorism as having three elements: being a criminal act; involving a transnational element, and done with the intent to spread fear among the population or directly or indirectly to coerce a national or international authority to take, or refrain from taking some action.[471] He also claims that this formulation of international terrorism complies with cyber terrorism in terms of unauthorized access to computer systems, but this definition is uncertain.[472]

The varying definitions suggest that cyber terrorist attacks involve fear, economic harm, political or social objectives and violence, with an ideological or political aim. To this, I would add the inflicting of economic damage and the threatening of many people in the international arena. By combining the above definitions, I would argue that cyber terrorism should be defined as a motivated attack by terrorists, attackers, or sub-national groups against target states using cyber space in order to harm and destroy national and international critical infrastructure, including communication, transportation, energy, security, SCADA and banking systems, as well as personal information, and the threatening people in the states and international arena for the purpose of achieving political, cultural, or economic aims. Article 3/f of the Stanford Draft states that, if there is an attack on one of the cyber systems mentioned in the international conventions against terrorism which it lists, that attack can be labelled cyber terrorism.[473]

Jalil mentions five types of cyber terrorist attack,[474] including:

[469] *Ibid*.,pp. 6-7

[470] *Ibid*.

[471] Fidler, D. P. (2014), "Overview of International Legal Issues and Cyber Terrorism", *International Law Association*, p. 8

[472] *Ibid*.

[473] Article 3/f of the Stanford Draft uses a cyber-system as a material factor in committing an act made unlawful or prohibited by any of the following treaties: (i) Convention on Offenses and Certain Other Acts Committed on Board Aircraft, September 14, 1963, 20 U.S.T. 2941 [Tokyo Convention]; (ii) Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking), December 16, 1970, 22 U.S.T. 1641 [Hague Convention]; (iii) Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), September 23, 1971, 24 U.S.T. 564 [Montreal Convention]; (iv) International Convention Against the Taking of Hostages, December 17, 1979, T.I.A.S. 11081 [Hostages Convention]; (v) International Convention for the Suppression of Terrorist Bombings, December 15, 1997, 37 I.L.M. 249 [Terrorist Bombings Convention]; (vi) United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, December 20, 1988, T.IA.S., 20 I.L.M. 493 [Vienna Convention on Narcotics]; (vii) International Maritime Organisation Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation [Maritime Terrorism Convention], March 10, 1988, IMO Doc. SUA/CON/15/Rev.1, 1993 Can. T.S. No. 10. Sofaer, and Goodmani, *op.cit*., p.28

[474] Jalil, S. A. (2003), "Countering Cyber Terrorism Effectively: Are We Ready To Rumble?", *SANS Institute*, Available at: http://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (Accessed at: 01/04/2015), p. 8

1) *Incursion*: the main aim of the cyber terrorist is to access a network in order to gain information or change the information in the systems to gain an advantage over others (e.g. stealing secret governmental or personal information);

2) *Destruction:* as can be understood from the name, the main aim of this type of attack is that of destroying or harming computer systems (e.g. the Estonian case);[475]

3) *Disinformation:* the aim of this type of attack is to create fear or chaos in the target state by means of rumours;

4) *Denial of Service:* a common cyber terrorist attack, the main aim of this type of attack is to lock online computer systems;

5) *Defacement of Websites:* as can clearly be understood, the main aim of this type of attack is the defacement of websites (i.e. a website's information can be changed by the attackers, thereby allowing the terrorists to conduct propaganda on those affected websites).

Zanini and Edwards classify cyber terrorism attacks in a narrow way, identifying three types of offensive information-operational activities with which technology can help cyber terrorists. These are, firstly, using the Internet for perception management and disseminating propaganda for the purpose of recruiting new members, funding the terrorist group and influencing public opinion; secondly, using the Internet and other computer systems to disrupt target systems (i.e. short disruptive attacks); and, lastly, using technology to destroy critical infrastructures, including air traffic control, water and power systems, etc.[476]

The Council of Europe has divided cyber terrorism into three different categories.[477] [478] Table 1 sets out this cyber incident typology.

[475] See Chapter 1

[476] Zanini, M. and Edwards, S. J. A. (2001), “The Networking of Terror in the Information Age,” in Arquilla, J. and Ronfeldt, D. (2001), *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica: RAND, pp. 41-46

[477] The document was prepared by Prof. Dr. Ulrich Sieber and Phillip W. Brunst.

[478] I am not going to explain all of the details regarding this cyber terrorist incident and its report. I will only try to provide a short explanation about this type of cyber incident.

Table 1: Cyber Incident Typology by the Council of Europe

A. Attacks via the Internet	B. Dissemination of Content	C. Use of the Internet for Other Purposes
1. Attacks on Infrastructure a) Types - Large Scale Attacks - Hacking Attacks - Hybrid Attacks - Attacks Resulting in Physical Damage	1. Presentation of Terrorist Views	2. Individual Communication
2. Attacks on Human Life a) Attacks Using Control Systems b) Long-Term Developments	3. Propaganda and Threats	4. The Internet as a Planning and Support Instrument
	5. Recruitment and Training	
	6. Fundraising and Financing	

Source: The Council of Europe (2008), *Cyber terrorism: The Use of The Internet for Terrorist Purposes*, Strasbourg: Council of Europe Publishing

The COE explains why terrorist organisations use the Internet or other information technologies as follows:

> - *Attacks can be launched from anywhere in the world. An internet connection is available at most locations or can be initiated from most up-to-date mobile phones;*
> - *Attacks are quick. Especially in cases of Distributed Denial-of-Service (DDoS) attacks, but also in many other scenarios, the attacker is not dependent on a fast internet connection speed of the victim. Worms and viruses can spread at the fastest possible rate without the need for any further involvement of the attacker;*
> - *Since actions on the internet can be disguised by anonymising services or using similar camouflage techniques, in many cases it is extremely difficult to trace evidence back to the true perpetrator;*

- *Finally, use of the Internet is cheap. In most cases, only small bandwidth connection is needed which is highly affordable in most countries.*[479]

By contrast, Ballard *et al.* seek to provide a comprehensive classification by dividing the typology of the concept of cyber terrorism into four different categories. These are specified in the following table.[480]

Table 2: Cyber Incident Typology

Category	**Definition or Explanation**
Information Attacks	Cyber terrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various materials therein.
Infrastructure Attacks	Cyber terrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programming in a computerized environment.
Technological Facilitation	Use of cyber communications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyber terrorism.
Fund Raising and Promotion	Use of the Internet to raise funds for a violent political cause, to advance an organisation supportive of violent political action, or to promote an alternative ideology that is violent in orientation.

Source: Ballard, J. D., Hornik, J. G. and McKenzie, D. (2002), "Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues", *American Behavioral Scientist*, Vol: 45(6), Available at: http://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1007&context=scjpeerpubs (Accessed at: 01/04/2015), p. 1009

According to Ballard *et al.*, information attacks can occur in several different ways. Some of them are explained above (e.g. defacement of websites and denial of service attacks). Another type of information attack is that of the *malicious code*, or Malware. This type of cyber incident includes three different styles: viz., Trojan horses, viruses and worms. Malware attacks can bring down information systems, causing the victim not to be able to use their operating systems temporarily.[481] The *Trojan horse* is explained by Bhagyavati as being: "*A malicious program that disguises itself as a safe application. Trojan horses do not replicate*

[479] The Council of Europe (2008), *Cyberterrorism: The Use of The Internet for Terrorist Purposes*, Strasbourg: Council of Europe Publishing, pp. 16-17

[480] Ballard, J. D., Hornik, J. G. and McKenzie, D. (2002), "Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues", *American Behavioural Scientist*, Vol: 45(6); Available at: http://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1007&context=scjpeerpubs (Accessed at: 01/04/2015), p. 1008

[481] Charvat, J. (2009), "Cyber Terrorism: A New Dimension in Battlespace," in Czosseck C. and Geers, K. (eds.) (2009), *The Virtual Battlefield Perspectives on Cyber Warfare*, Amsterdam: IOS Press, p. 84

themselves, but they are as damaging to a computer system as viruses, which replicate themselves."[482] The main aim of Trojan horses is to damage computer systems, with Trojan horses accessing important information and changing it. *Viruses*, on the other hand, are explained by Mishra and Mishra as being: "*A malicious code added to an e-mail program or other downloadable file that is loaded onto a computer without the users [sic] knowledge and which runs often without their consent. Computer viruses can often copy themselves and spread themselves to a user's e-mail address book or other computers on a network.*"[483] An example of the impact a virus can have was the I LOVE YOU virus, [484] which affected the whole international community on 4 May 2000, causing an estimated 8.7 billion US dollars in damages.[485] And finally, *worms* are another type of malicious code used in information attacks. Worms can exist as a separate programme in a computer and do not need to attach themselves to other programmes. According to Wilson, worms will drag up any computer on the internet which has vulnerabilities in order to rapidly install themselves onto the victim's computer so as to attack it.[486]

One of the other cyber incident types identified by Ballard is infrastructure attacks. According to Jalil, "*[t]he cyber terrorists generally perceive their targets to be either high-profile components of a nation's critical infrastructures or business operations. The main objective of these terrorists is to inflict damage which will either compromise or destruct targets in order to cause major physical and psychological impacts to them.*"[487] Hardy and Williams emphasise that this type of attack may cause economic chaos, massive loss of life, and environmental damage. Air traffic control systems, nuclear power stations, SCADA, hospitals, and any other critical system may be targeted by cyber terrorists, in order to either damage or have more influence on society.[488] For example, Turkey recently faced a cyber-attack in its energy centres on 31 March 2015, affecting many cities, including the major

[482] Bhagyavati, B. (2008), "Social Engineering," in Janczewski, L. J. and Colarik, A. M. (eds.) (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference, p. 190

[483] Mishra, A. and Mishra, D. (2008), "Cyber Stalking: A Challenge for Web Security," in Janczewski, L. J. and Colarik, A. M. (eds.) (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference, p. 224

[484] Seltzer, L. (2010),*'I LOVE YOU' Virus Turns Ten: What Have We Learned?*, Available at: http://www.pcmag.com/article2/0,2817,2363172,00.asp (Accessed at 02/10/2015)

[485] "Dünya'nın En Etkili Bilgisayar Virüsleri,", Available at: http://www.milliyet.com.tr/fotogaleri/44071-yasam-dunyanin-en-tehlikeli-bilgisayar-virusleri/6 (Accessed at: 02/04/2015)

[486] Wilson, C. (2005), "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress," *CRS Report for Congress*, Available at: http://fpc.state.gov/documents/organisation/45184.pdf (Accessed at: 01/04/2015), p. 39

[487] Jalil, *op.cit.*, p. 4

[488] Hardy and Williams, *op.cit.*, p. 1

cities of, Ankara, İstanbul and İzmir.[489] As a result, officials (and people in general) talked about cyber-attacks on Turkey's electric grids. Many of Turkey's cities did not use electricity for more than 10 hours because of the attacks on the electric grids.[490]

Cyber-attacks are not unpredictable, but the place, time and effect on society, on the other hand, can be unpredictable.[491] Some countries, such as the USA and the UK, have invested heavily in recruiting cyber infrastructure securities. This situation, however, is not equal when one compares them with other states in terms of spending capacity to improve their infrastructure securities. The cyber-attacks on Estonia demonstrate the reality of this threat and problem.

Technological facilitation, which is the third cyber terrorist attack type identified by Ballard *et al.*, concerns using the Internet for the purpose of catalysing terrorism or cyber terrorism;[492] in other words, they wish to shape terrorist organisations and create flexible communications between terrorists. The UN highlights the fact that the Internet is one of the most effective types of communication between terrorists, mentioning that "*a simple online e-mail account may be used by terrorists for electronic, or virtual, 'dead dropping' of communications. This refers to the creation of a draft message, which remains unsent, and therefore leaves minimal electronic traces, but which may be accessed from any Internet terminal worldwide by multiple individuals with the relevant password.*"[493] By encrypting their messages, terrorists can communicate with one another freely and without fear. Lesce explains that "*this emerging trend is worrisome to counterterrorism professionals*"[494] Lachow describes this situation as follows:

> *"Modern encryption technologies allow Internet users to surf the Web, transfer funds, and communicate anonymously—a serious (though not*

[489] "Elektrik Kesintisi: Türkiye Bir Gün Elektrik Alamadı", Available at: http://www.bbc.com/turkce/haberler/2015/03/150331_elektrik_rengin (Accessed at: 02/10/2015)

[490] "Taner Yıldız: Siber Saldırı mıdır? Söyleyemem!", Available at: http://www.radikal.com.tr/turkiye/taner_yildiz_siber_saldiri_midir_soyleyemem-1325196 (Accessed at: 01/04/2015); See also; "79 İlde Elektrik Kesintisinin Nedeni Siber Saldırı mı?", Available at: http://www.aktifhaber.com/79-ilde-elektrik-kesintisinin-nedeni-siber-saldiri-mi-1147527h.htm (Accessed at: 01/04/2015). Also "Elektrik Kesintisinin Nedeni Siber Saldırı mı", Available at: http://www.cnbce.com/haberler/turkiye/elektrik-kesintisinin-nedeni-siber-saldiri-mi (Accessed at: 01/04/2015). And "Türkiye'de Büyük Çapta Elektrik Kesintisi: Siber Saldırı İhtimali Araştırılıyor", Available at: http://tr.sputniknews.com/turkiye/20150331/1014730458.html (Accessed at: 01/04/2015)

[491] Ellyatt, H. (2015), *Cyberterrorists to Target Critical Infrastructure*, Available at: http://www.cnbc.com/id/102367777 (Accessed at: 01/04/2015)

[492] Ballard and *et. al.*, *op.cit.*, p. 1010

[493] The United Nations Office on Drug and Crime (2012), *The Use of the Internet for Terrorist Purposes*, United Nations: Vienna, Available at: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (Accessed at: 05/05/2015), p. 24

[494] Ballard *et al.*, *op.cit.*, p. 1010

> *insurmountable) impediment to intelligence and law enforcement organisations trying to find, track, and catch terrorists. To do this, terrorists can download various types of easy-to-use computer security software (some of which is commercial and some of which is freely available) or register for anonymous email accounts from providers like Yahoo! or Hotmail."*[495]

In accordance with this information, it can be said that technological facilitation consists of the encryption of messages, the sharing of information via e-mails, the dissemination of information and the use of websites for propaganda purposes.

The last cyber incident type is that of fundraising and promotion. According to the UN, the raising and collecting of funds and resources can be classified into four categories.[496] First, there is direct solicitation. This uses internet sources such as chat groups, websites and so on to request donations from their supporters.[497] The second category is e-commerce, which includes the selling of books, audio, or other items to their supporters from terrorist organisation websites (or other related websites).[498] The third type is the exploitation of online payment tools (i.e. fraud). Terrorists are able to steal identities and credit cards and conduct auction fraud.[499] As one UN document states:

> *"…the use of gains to finance acts of terrorism can be seen in the United Kingdom case against Younis Tsouli. Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which were used to route the funds through several countries before they reached their intended destination. The laundered money was used both to fund the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity."*[500]

[495] Lachow, I. (2009), "Cyber Terrorism: Menace or Myth?", in Kramer, F. D., Starr, S. H. and Wentz, L. K. (2009), *Cyberpower and National Security*, Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-19.pdf (Accessed at: 08/05/2015), p. 14

[496] The United Nations Office on Drug and Crime, *op.cit.*, p. 7

[497] *Ibid.*

[498] *Ibid.*

[499] *Ibid.*

[500] *Ibid.*

The last, or fourth type includes using charitable organisations for raising funds and obtaining promotions. Examples include the Benevolence International Foundation, Global Relief Foundation, and the Holy Land Foundation for Relief and Development[501], which have all have been used as a front to finance terrorist organisations and promote their ideologies.

Walker has his own typology, the importance of which to use information warfare under cyber terrorism. Doğrul *et al* argue that cyber terrorism and information warfare are different concepts.[502] As stated above, cyber terrorism can be defined as politically motivated attacks against information and computer systems and can result in violence against non-combatants,[503] but, on the other hand, Janczewski and Colarik explain information warfare as being "*...a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses.*"[504] Also, Rona, who first mentioned the concept of information warfare in the international arena,[505] describes it as:

> *"The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives."*[506]

I suggest that this definition is too broad to explain information warfare. Even though it refers to there being competition between two or more states or parties in terms of improving their security capabilities with strategy, operations, or tactics, information warfare is much more complex. *"It subsumes most human activity…Information war exists to ensure that one's own picture of a conflict is more correct than that held by the other side. This perspective is useful but incomplete. All viewpoints are incorrect, because data cannot be incorporated without a conceptual structure to hang them on. Yet even the best structures are abstractions of a complex world. Whether the structures are biased in important and harmful or trivial and harmless ways is what matters."*[507] Whilst Rona's

[501] *Ibid.*

[502] Doğrul, M., Aslan, A. and Çelik, E. (2013), "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism", *2011 3rd International Conference on Cyber Conflict*, Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf (Accessed at: 25/07/2016), p. 31

[503] *Ibid.*

[504] Janczewski, L. J. and Colarik, A. M. (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference, p. xiv

[505] Geers, K. (2011), *Strategic Cyber Security*, Tallinn: CCDCOE Publications, p. 25; Cavelty, M. D. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Oxon: Routledge, p. 44; Gray, C. S. (2006), *Another Bloody Century: Future Warfare*, London: Phoenix

[506] Libicki, M. C. (1995), *What is Information Warfare?*, The Centre for Advanced Concepts and Technology, p. 4

[507] *Ibid.*

definition is broader, Janczewski and Colarik's definition is much sharper, and helps to explain the concept of information warfare in its present conditions.

Although Walker evaluates information warfare under the typologies of cyber terrorism, the definitions show us that information warfare is different and should be analysed under its current conditions.

Today, when we think about terrorist organisations, they have their own multilingual websites. Thus, they are able to raise funds and promote their ideologies throughout the entire world. For example, Al-Qaeda has many websites and has founded charities, non-governmental organisations, chat groups, etc., for the purpose of raising funds and promoting its ideology to others.[508] More recently, ISIS has tried to improve its capability on the Internet by using internet tools for fundraising, promoting its ideology and inducting new members.[509] It seems that the COE's cyber incident typology is similar to that of Ballard *et al*., the main difference between them being that the COE accepts that one of the most important cyber incidents concerns human life. If the cyber terrorists' activities cause fear in societies, the attacks become more effective; this, in turn, means that people may start to feel that they are at risk of cyber-attacks if they occur repeatedly.[510] From this viewpoint, civilians may be the target of cyber-terrorist actions which affect their lives. As is commonly known, civilians are frequently the target of cyber terrorist activities in terms of identity theft or fraud, but threats to human life are different from all of these. So, even though the COE's explanation of the typology of cyber incidents is more comprehensive than Ballard *et al.*'s, both can be used by researchers in order to explain the typology of cyber terrorism in detail.

2.5.4.1. The Attributes of Cyber Terrorists: Who are Cyber Terrorists?

Having described what cybercrimes and cyber terrorism are, I now turn to identifying and defining cyber terrorists. There are many people who commit cybercrime, including hackers, rogues and robbers who cannot be characterised as cyber terrorists. For instance, according to Elazari, some hackers are actually attempting to help us fix our world[511] by closing the gaps in the virtual world enabling others to use the Internet and information security safely.

[508] Weimann, G. (2004), *How Modern Terrorism Uses the Internet*; Available at: http://www.usip.org/sites/default/files/sr116.pdf (Accessed at: 08/05/2015); See also; Kaplan, E. (2009), Terrorists and the Internet, *Council on Foreign Relations*, Available at: http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p1 (Accessed at: 08/05/2015)

[509] Irshaid, F. (2014), *How ISIS is Spreading Its Message Online*, Available at: http://www.bbc.com/news/world-middle-east-27912569 (Accessed at: 08/05/2015)

[510] *Ibid*., p. 29

[511] Elazari, K. (2014), *Hackers: The Internet's Immune System*, Available at: https://www.ted.com/playlists/10/who_are_the_hackers (Accessed at: 12/05/2015)

However, if the hackers' motivation is that of raising money, promoting an ideology, or harming critical infrastructures, these hackers may, indeed be called cyber terrorists.[512]

From this viewpoint, it can be said that those who use the Internet effectively for the purpose of attacking a government with a malicious aim can be considered cyber terrorists.

2.6. Conclusion

The definition of the term "threat" has changed over time, and some historical background has been provided above to show this. In ancient times, the concept changed with the changes to security policies. Together with the development of international relations, international law and, most importantly, philosophy and theories, the concept has been defined in different ways, and because of this, there is no common definition of the concept.

The concept of threat can be summarised as the negative consequences of a policy on the states or on international peace and security. It may be accepted that, throughout history, certain policies have been perceived as threats by other states, such as increasing of security policies, and this situation continues. In recent times, if a state has nuclear weapons, or is likely to produce them, this will be taken as a threat by any neighbouring states. Ultimately, the determination of threat perceptions may be based on the political aims of the big states and organisations.

With the development of different theoretical approaches, new policies emerged in the international arena. Wars, conflicts, terrorism and some security policies have been regarded as threats by the international community, but with the development of collective security, new threat perceptions are accepted as being a threat to international peace and security.

NATO's purpose changed after the collapse of the USSR. After 1990, NATO tried to produce adopt itself to post-Cold War era and the organisation has changed its structure from threat to risk. The new paradigm has allowed the organisation to survive its ability in the international arena and with this new shift, new policies against risks and threat perceptions have been accepted by NATO. Along with NATO, the United Nations recognised new perceptions of threats to international peace and security as:

[512] Lawson, S. M. (2002), *Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure,* Available at: http://www.sans.org/reading-room/whitepapers/warfare/information-warfare-analysis-threat-cyberterrorism-critical-infrastruc-821#__utma=183869984.1510179836.1427206897.1427206897.1427206917.2&__utmb=183869984.1.9.1427223458399&__utmc=183869984&__utmx=-&__utmz=183869984.1427206897.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=-&__utmk=175029154 (Accessed at: 12/05/2015)

- Economic and social threats, including poverty, infectious disease and environmental degradation
- Inter-State conflict
- Internal conflict, including civil war, genocide and other large-scale atrocities
- Nuclear, radiological, chemical and biological weapons
- Terrorism
- Transnational organized crime. [513]

The development of technological improvements has allowed attackers, terrorists, or other people who are able to use technological tools to achieve their goals using information technologies to harm or create fear in societies for their own interests this includes stealing identities, credit cards, committing fraud, or attacking states' critical infrastructures. The Estonian attack remains the most significant example not just in terms of the impact they had on the country but also in terms of identifying these new threat perceptions and state and international organisations policies against them.

In conclusion, the determination of threat perceptions and risks change from state to state, and therefore it is necessary to determine collective risk and threat perceptions in the area, without considering political aims and interests. Stronger states have used their powers to identify threat perceptions and risks within their strategic concept, position or interest in the international community, as well as in international organisations. This situation makes the identification of the threat perceptions contradictory.

Lastly, these new risks and threat perceptions may have more potential to harm and create fear in societies. We live in what Ikuenobe describes as an "*information jungle, the Wild West, where everyone has easy, free, and quick access to all sorts of information - good and bad, false and true*".[514] Although, logically, more information is understood to enhance the lives of citizens, in fact, the greater the amount of information, the harder it may become to identify specific cyber-attacks. It is difficult to distinguish the good from the bad. It is expensive to monitor all incoming information in order to safeguard the state and protect the individual. This has obvious problems for states and international institutions. A considerable amount of money, time and expertise are needed to put protection in place and simply evaluate and process data. This raises issues about how to decide what strategies to adopt – what

[513] Report of the High-Level Panel on Threats, Challenges and Change, United Nations, *op.cit.*, p.2

[514] Ikuenobe, P. (2003), "Optimising Reasonableness, Critical Thinking and Cyberspace", *Education Philosophy and Theory*, Vol. 35 (4), p. 408

criterion(a) should be considered? This is a problem for the institutions and also raises legal questions about the nature of information and the method or criteria for determining if it is credible enough to base a reasonable decision to act, or not to act upon**.**

CHAPTER 3: GAME THEORY

3.1. Introduction

Game Theory is important in this research, because the theory analyses interactive or independent situations, using models with clear statements of outcomes which depend on the action taken by more than one individual.[515] Also, Game Theory analyses the decisions of two or more people, and offers strategies for both sides to have more outcomes in the game. Moreover, as Matusitz states, "*the cyber-attacker and the computer security agent not only engage in real-time game play but also use strategies that are not conceivable in conventional warfare. For this reason, the theory can greatly contribute to a better understanding of cyber strategy and its implications*."[516] In short, the theory helps to understand the strategies of both sides, which are the cyber-terrorists/attackers and the states or international organisations, and their behaviours towards and possible interactions with each other.

Myerson considers that the development of the theory began with the work of Zermelo (1913), Borel (1921) and von Neumann (1928), and with the book, Theory *of Games and Economic Behaviour*, by von Neumann and Morgenstern (1944).[517] Since its inception, Game Theory has evolved and found a suitable mould to implement itself in science and social sciences. As a result, it has been applied to economics, political sciences, law, mathematics and other sciences.[518]

Game Theory deals with decision-making in conflict situations[519] for minimizing the maximum possible loss, or maximizing the minimum payoff in a game, political arena, or economy. The Game Theory generally analyses rational behaviour, using mathematical tools

[515] Matusitz, J. (2009), "A Postmodern Theory of Cyberterrorism: Game Theory", *Information Security Journal: A Global Perspective*, Vol. 18 (6), Available at: http://www.tandfonline.com/doi/pdf/10.1080/19393550903200474?needAccess=true (Accessed at: 01/07/2016), p. 274

[516] *Ibid*.

[517] Myerson, R. (2001), *Game Theory Analysis of Conflict*, Cambridge: Harvard University Press, p.1

[518] Bilbao, J., Fernandez, J., Jimenez, N., and Lopez, J. (2002), "Voting power in the European Union Enlargement", *European Journal of Operational Research*, Vol. 143, Available at: http://www.esi2.us.es/~mbilbao/pdffiles/enlargue.pdf (Accessed at: 06/08/2015), p. 143, Also see, Fent, T., Feichtinger, G., and Tragler, G. (2002), "A dynamic game of offending and law enforcement", *International Game Theory Review*, Vol. 4(1), pp. 71–89

[519] Fuka, J., Obrsalova, I., and Langasek, P. (2012), "Game Theory Application on Terrorism", *Advances in Economics, Risk Management, Political and Law Science*, Available at: http://www.wseas.us/e-library/conferences/2012/Zlin/EPRI/EPRI-37.pdf (Accessed at: 03/01/2016), p. 229

or tables to understand and analyse its processes,[520] holding that all players have to be "*rational*" and have "*strategies*" to win, or to earn more payoffs. Matusitz explains Game Theory as "*Game theory analyses rational behaviour in interactive or interdependent situations and proposes a set of mathematical tools and models for analysing these interactive or interdependent processes*."[521] All players of these games would assume that the reduction of their loss in a conflict area would mean gaining advantages or income/payoff over the other players. According to Matusitz, "*Since games frequently reproduce or share characteristics with real situations, they can offer strategies for dealing with such circumstances*".[522] Moreover, all sides of the game have their own strategies, one of which is represented by the attacker, who desires to have greater influence in the society, and the other, which is protecting its systems from attack. The number of players does not matter, and each player is also a decision-maker and creator of new strategy in the game. Because each player seeks to achieve more outcomes and effects, their strategy or moves will give a result for both sides.[523] According to Rapoport, each player has to find a new way to gain more outcomes against his or her opponents. This means that each player has to employ strategic thinking about the next step of his/her moves, and to consider how his/her payoffs will impact the other players.[524]

Also, different outcomes are possible in Game Theory. Simply defined, Cooperative Game Theory can have coalitions and combine their decisions to have more outcomes in the game.[525] Brandenburger states that Cooperative Game Theory can be described only when the players come together in different combinations to have a result in the game, and is not just cooperation that has materialized among the players. It also includes competition in a strong form.[526] On the other hand, Non-Cooperative Game Theory is based on the analysis of

[520] Neel, J. J. (2005), "Game Theory can be used to analyze cognitive radio", *Electronic Engineering Times*, 1386, pp. 69–72;, Poundstone, W. (1993), *Prisoners Dilemma*, New York: Anchor Books, p.44; Pavel, L. (2012), *Game Theory for Control of Optical Networks*, New York: Springer Science+Business Media, p. 11

[521] Matusitz, *op.cit.*. p. 274

[522] Matusitz, *op.cit.*. p. 274

[523] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandiya, V. and Wu, Q. (2011), "A Survey of Game Theory as Applied to Network Security", *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences*, Available at: http://ais.cs.memphis.edu/files/papers/Survey.pdf (Accessed at: 25/07/2016), p. 2

[524] Rapoport, A. (*Ed*.) (1974), *Game Theory as a Theory of Conflict Resolution*, Boston: D. Reidel Publishing Company, p. 86

[525] Chalkiadakis, G., Elkind, E. and Wooldridge, M. (2012), "Cooperative Game Theory: Basic Concepts and Computational Challenges", *IEE Intelligent Systems*, Available at: http://www.cs.ox.ac.uk/people/michael.wooldridge/pubs/ieeeis2012d.pdf (Accessed at: 05/09/2016), p. 86

[526] Brandenburger, A. (2007), Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution, Available at: http://www.uib.cat/depart/deeweb/pdi/hdeelbm0/arxius_decisions_and_games/cooperative_game_theory-brandenburger.pdf (Accessed at: 05/09/2016), p. 1

strategic choices by the players. The interests of the player take a main role in Non-Cooperative games. According to Turocy and Stengel, cooperation in the Non-cooperative game models can be possible when the players maintain their best interests.[527]

Before explaining its assumptions, definitions of the terms used in Game Theory are explained for better understanding. Roy *et al* define these terms as:

- *Game*: A description of the strategic interaction between opposing, or co-operating, interests where the constraints and payoff for actions are taken into consideration.
- *Players*: A basic entity in a game that is tasked with making choices for actions. A player can represent a person, machine, or group of persons within a game.
- *Strategy*: Plan of action within the game that a given player can take during game play.
- *Payoff*: The positive or negative reward to a player for a given action within the game.[528]

3.2. The Types of Game Theory

3.2.1. Nash Equilibrium

Nash Equilibrium is a cornerstone of the Game Theory and was introduced by John Nash.[529] According to Nash Equilibrium, both sides in a game will take action against each other, but one of them takes the best and most important action compared with the others.[530] The main aim of the game or action is that each player has to make the best decision to have more outcomes against his/her opponents. At the end of the game, both sides will have some outcomes, but one of them will have more than others. This is to say that each player aims to maximize his/her own payoffs. This strategy can be a combination of decisions with any other players in the game. The key point in the Nash Equilibrium is that each player has to use other players' strategies, as given in the game to take best possible action.[531] According to Fudenber and Tirole, if a player wants to change his/her own strategy to gain more payoffs, this will not be effective against his/her opponents, and the player cannot gain anything in

[527] Torucy and Stengel, *op.cit.,* p. 7
[528] Roy, *et al., op.cit.*
[529] Myerson, *op.cit.,* p. 105. Also see for more information, Mehlmann, A. (2000), *The game's afoot! Game Theory in myth and paradox*, Providence, RI: American Mathematical Society
[530] Mehlmann, *Ibid*.
[531] Nash, J. (1950), "Equilibrium Points in N-Person Games", *Proceedings of the National Academy of the USA*, Vol. 36(1), pp. 48–49

terms of outcomes. For example, if a player has a strategy and does not want to change it to gain more payoffs, the other players use the same strategy and the outcomes or payoffs create a Nash Equilibrium.[532]

Easley and Kleinberg state that the idea of the Nash Equilibrium is that “*if the players choose strategies that are best responses to each other, then no one can change its strategy and the system is in a kind of equilibrium state*.[533] In short, Nash equilibrium is a combination of players’ strategies where both sides use each other’s strategy to take best action against the other side and gain more payoffs.[534] Some examples can be given of Nash equilibrium to explain it in detail. Turocy and Stengel use the high-low quality game to explain Nash equilibrium.

		Player 2	
		Buy	**Do not buy**
Player 1	**High**	**2, 2**	**0, 1**
	Low	**1, 0**	**1, 1**

Table 3: High-Low quality game[535]

According to Table 3, when Player 1 produces high quality service, Player 2 buys this service. But when Player 1 produces low quality service, Player 2 does not buy this service. There are two different Nash Equilibria here. One is low-do not buy, and another is high-buy. The first equilibrium has fewer payoffs than the second choice, and the second equilibrium, which is the high-buy strategy, is a more desirable solution for the players.[536]

Another example is adopted from the works of Easley and Kleinberg.[537] According to Easley and Kleinberg, there are two different firms and they would like to do business with one of three large clients, A, B and C. Each firm has three possible strategies and the results of their two decisions work out as follows:

[532] Fudenberg, D. and Tirole, J. (1991), *Game Theory*, Cambridge, MA: MIT Press, pp. 11-14, Also see, Poundstone, *op.cit*., p. 98

[533] Easley, D. and Kleinberg, J. (2010), *Networks, Crowds, and Markets: Reasoning About A Highly Connected World*, Cambridge: Cambridge University Press, p. 150

[534] Colman, A. M. (2003), *Game Theory and Its Applications: In the Social and Biological Sciences*, London: Routledge, p. 59

[535] The numbers are chosen randomly. Also first numbers belong to player 1 and second numbers belong to player 2.

[536] Turocy, T. L. and Stengel, B. V. (2001), *Game Theory*, Available at: http://www.cdam.lse.ac.uk/Reports/Files/cdam-2001-09.pdf (Accessed at: 01/09/2016), p. 13

[537] I adapted this example completely from the Works of Easley and Kleinberg.

- *If the two firms approach the same client, then the client will give half its business to each.*
- *Firm 1 is too small to attract business on its own, so if it approaches one client while Firm 2 approaches a different one, then Firm 1 gets a payoff 0.*
- *If Firm 2 approaches client B or C on its own, it will get their full business. However, A is larger client, and will only do business with the firms if both approach A.*
- *Because A is a larger client, doing business with it is worth 8 (and, hence, 4 to each firm, if split), whereas doing business with B or C is worth 2 (and hence 1 to each firm if split).*[538]

Firm 2

		A	**B**	**C**
Firm 1	**A**	4, 4	0, 2	0, 2
	B	0,0	1, 1	0, 2
	C	0,0	0, 2	1, 1

Table 4: Three-Client Game

It is clear that there is one Nash equilibrium in the table, which is the A, A strategy. It is mentioned above that the Nash equilibrium is the best response to the other players' responses and when the table evaluated the best response for Firm 1, it chose the client A. On the other hand, A is also the best strategy for Firm 2 against Firm 1. Other strategies do not have best responses to each other and therefore there is only one Nash Equilibrium here.
it is clear from the examples that the best response is important in the Nash Equilibrium and the players try to use their best strategies with other players.

3.2.2. Coordination games

Coordination games are defined by Colman as: "*an agreement among the players as to their preferences among the possible outcomes; in particular, an outcome that is considered best*

[538] Easley and Kleinberg, *op.cit*., pp. 149-150

by one player is considered best by the others.”[539] Colman’s approach on the coordination games is explained under Pure Coordination Games. There is no conflict of interest between the players of Pure Coordination Games, and their main aim is to coordinate their strategies in the game.[540] Colman’s Head On game is one example of a Pure Coordination Game. According to Colman, there are two people and they are walking in the same corridor towards each other; if they continue to walk towards each other, they will collide. They have three different strategies, which are to swerve left, swerve right or keep going straight ahead. If they both choose to swerve to the same side of the corridor or keep going straight ahead, they will collide, but in other conditions, such as one swerving to the right and the other keeping going straight ahead or vice versa, they will not collide.[541] Easley and Klienburg state that “*the outcome of the game depends on the decisions of both walkers whose interest coincide exactly inasmuch as their preferences among the outcomes are identical*.[542]” It is clear that they will need coordination to have more outcomes, and their preferences among the outcomes are identical.

Easley and Kleinberg also identify Unbalanced Coordination Games, and these games have two Nash equilibria.[543] They give an example of Unbalanced Coordination Games as:

		Player 2	
		PowerPoint	**Keynote**
Player1	**PowerPoint**	1, 1	0, 0
	Keynote	0, 0	2, 2

Table 5: Unbalanced Coordination Game[544]

Table 5 illustrates that two players would like to prepare slides for their work, but there are two different types of software to prepare these slides. If Player 1 chooses to use PowerPoint and Player 2 chooses keynote, they will have low payoffs. Also, it is clear that there are two Nash equilibria in the table: PowerPoint-PowerPoint and Keynote-Keynote. If they use the other player’s software, it will be much easier to prepare and merge the documents. If both choose different software, a problem will occur and coordination will not be unobtainable.

[539] *Ibid*., p. 33
[540] *Ibid*., p. 35
[541] *Ibid*., p. 3
[542] Ibid., p. 4
[543] Easley and Kleinberg, *op.cit.*, p. 151
[544] This table is adapted from the work of Easley and Kleinberg. *Ibid*.

Easley and Kleinberg explain the use of Schelling's idea on how this difficulty can be solved. According to them, "*Thomas Schelling introduced the idea of a focal point as a way to resolve this difficulty. He noted that in some games there are natural reasons (possibly outside the payoff structure of the game) that cause the players to focus on one of the Nash equilibria. For example, suppose two drivers are approaching each other at night on an undivided country road. Each driver has to decide whether to move over to the left or to the right. If the drivers coordinate – making the same choice of side–then they pass each other, but if they fail to coordinate, then they get a severely low payoff due to the resulting collision. Fortunately, social convention can help the drivers decide what to do in this case: if this game is being played in the United States, convention strongly suggests that they should move to the right, where as if the game is being played in England, convention strongly suggests that they should move to the left. In other words, social conventions, while often arbitrary, can sometimes be useful in helping people coordinate among multiple equilibria*."[545] In short, social conventions or communications help people to coordinate for the best payoff.

One of the other variations of the coordination game is the Stag Hunt game which is based on the writing of Rousseau.[546] According to the story, there are two hunters, and if they cooperate, they will hunt a stag which will be the highest payoff outcome for them, but if they do not cooperate and choose their own interests, they will catch the hare. The preferred game is hunting the stag, but the tricky part of the game is that if one of them tries to hunt a stag, he will not catch anything else, but if another hunter does not cooperate with him or her, and tries to hunt a hare, he or she will able to catch the hare, and this hunter will have more payoff than first hunter. The payoffs are shown in Table 6, and this game is a little similar to Unbalanced Coordination Game, but the difference is that if two players coordinate differently, one will have higher payoff than another player.[547] The game also has two equilibria in Stag-Stag and Hare-Hare. The problem in the table or stag hunt is that stag-stag strategy is more risky than hare-hare strategy. The risk point of the stag-stag strategy, as mentioned above, is that if one tries to hunt a stag, but the other does not coordinate with him or her, one will have 0 payoffs and another will have 3 payoffs. Therefore, these hunters will

[545] *Ibid*.

[546] Skyrms, B. (2004), The Stag Hunt and The Evolution of Social Structure, Cambridge: Cambridge University Press, p. 1

[547] Easley and Kleinberg, *op.cit*., p. 153

choose a less risky strategy, which is the hare-hare strategy.[548] It is important to explain why the hunters chose less payoff strategy than greater payoff strategy. As explained above, coordination is important in the game, and if one of them coordinates differently and chooses another strategy, the payoff will be 0 and therefore the hunters chose the hare-hare strategy.

According to Easley and Kleinberg, there are some differences between Prisoners' Dilemma and the Stag Hunt game. For example, Prisoners' Dilemma has dominant strategies, but on the other hand, if the players of the Stag Hunt game cooperate with each other, their benefit will be greater, but the risk is changed if one tries to cooperate, while his or her partner does not cooperate.[549]

		Player 2	
		Stag	**Hare**
Player1	**Stag**	4, 4	0, 3
	Hare	3, 0	3, 3

Table 6: Stag Hunt Game

The Battle of the Sexes game is also an important example of conflict interest in the coordination game. There is a couple, one man and one woman. They would like to spend more time with each other, and there are two options open to them. The man wants to go to a football match, but the woman wants to go to the theatre.

[548] McAdams, R. H. (2009), "Beyond the Prisoners' Dilemma: Coordination, Game Theory, and the Law", *Southern Law Review*, Vol. 82 (209), Available at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2648&context=journal_articles (Accessed at: 03/09/2016), pp. 220

[549] Easley and Kleinberg, *op.cit*., p. 153

		Woman	
		Football	**Theatre**
Man	**Football**	**4, 1**	**0, 0**
	Theatre	**0, 0**	**1, 4**

Table 7: The Battle of the Sexes Game [550]

Table 7 illustrates the Battle of the Sexes game, showing the worst and best outcomes for each player. There are two pure strategies or equilibria in the table as football-football and theatre-theatre. There is a conflict here, because the man chooses football-football, and the woman chooses theatre-theatre. Also, there is no similar strategy like in Prisoners' Dilemma in the Battle of the Sexes game. Communication can facilitate coordination, but if communication fails, then both players can choose their intended preferences. [551] Communication also provides bargaining power in the Battle of the Sexes, and McAdams evaluates the Battle of the Sexes game under this bargaining. According to McAdams, "*a bargain is possible only because two or more parties can mutually gain by some agreement… The problem is one of coordination because there is more than one way to conclude agreement and each party shares the desire to avoid an impasse that may result when each party presses for its preferred distribution…the Battle of the Sexes game captures what both sides know is the last round of bargaining, in which side will make its final offer and there are just two unequal ways for the offers to match. If the two offers match, there is a contract and both parties gain. If there is no match, the bargaining ends without an agreement and both parties lose. But each prefers to match terms in a different way*." [552] Although communication is essential in the Battle of the Sexes game, if one of them persists in using his or her strategy, communication can fail and both sides will choose their own preferences.[553]

[550] The numbers are chosen randomly. Also first numbers belong to player 1 and second numbers belong to player 2.

[551] Gooree, J. K. and Holt, C. A. (2000), "Coordination Games", *Encyclopedia of Cognitive Science*, Available at: http://www.econ.uzh.ch/dam/jcr:ffffffff-d693-da45-0000-00007653d068/CG.pdf (Accessed at: 03/09/2016), p. 4

[552] McAdams, *op.cit.*, pp. 236-237

[553] Cooper, R., DeTong, D. V., Forsythe, R. and Ross, T. W. (1989), "Communication in the Battle of the Sexes Game: Some Experimental Results", *The RAND Journal of Economics,* Vol. 20 (4), Available at: http://www.jstor.org/stable/pdf/2555734.pdf (Accessed at: 03/09/2016); Cooper, R., DeTong, D. V., Forsythe, R. and Ross, T. W. (1993), "Forward Induction in the Battle-of-the-Sexes Games", *The American Economic*

3.2.3. Two Person Zero-Sum Game

Two-person zero-sum game is one of the other types of Game Theory. According to this game, the interests of players are different, and they use diametrically opposed strategies to have more outcomes.[554] This means that if one player can gain more outcomes, others have to lose in the game. This situation creates balance, and the total balance will be Zero-Sum. Zero-Sum Game is similar to real wars, in that when one side wins the war, the other side loses and forfeits their territories. Von Neumann's approach to the Zero-Sum Game is generally based on two players and these games are necessarily non-cooperative.[555] Also, Colman states that if there are just two players, their interests are opposed, and they cannot use mutually profitable collaboration, therefore two-person zero-sum games are regarded as strictly competitive games.[556] Colman also gives some examples of two-person zero-sum games, such as economic, political, or military conflicts, political parties competing for votes and indoor games.[557]

Von Neumann developed a simple plan for deciding rational solutions of games. It is called the Minimax principle.[558] According to this principle, each player has a rational solution, and if a player is losing a game, he/she will aim to minimize his/her losses, while the other side will have a different strategy to gain more outcomes or maximize his/her payoffs. Most games, such as war-games, poker, etc. are Zero-Sum.

3.3. Prisoners' Dilemma

The Prisoners' Dilemma is one of the most famous games in the Game Theory.[559] Prisoners' Dilemma is usually explained with this example: there are two people and they have committed a crime. The police arrested them and placed in two different rooms to question them. There is no evidence for this crime unless one of them confesses or testifies against the other.

Review, Vol. 83 (5), Available at: https://www.jstor.org/stable/pdf/2117562.pdf (Accessed at: 03/09/2016); Easley and Kleinberg, *op.cit.*, p. 153

[554] Neumann, J. von and Morgenstern, O. (1944), *Theory of Games and Economic Behavior*. Princeton, NJ: Princeton University Press, pp. 238-242

[555] Poundstone, *op.cit.*, p. 97

[556] Colman, *op.cit.*, p. 53

[557] *Ibid.*, pp. 53-54

[558] *Ibid.*, p. 52

[559] Brams, S. J. (1993), "Theory of Moves", *American Scientist published by Sigma Xi*, Vol. 81, Available at: https://www.acsu.buffalo.edu/~fczagare/Game%20Theory/Theory%20of%20Moves.pdf (Accessed at: 28/07/2016), p. 565

		Player 2	
		Confess	**Disclose**
Player 1	**Confess**	**2, 2**	**0, 5**
	Disclose	**5, 0**	**1, 1**

Table 8: A Prisoners' Dilemma Game[560]

The police told both of them to cooperate and agree to confess/testify against the other player. If Player 1 confesses, and the other does not confess, then Player 1 will go free, whilst Player 2 will undergo long-term punishment for 5 years. If both confess, they will have 2 years punishment, and if both disclose the crime, they will have punishment reduced to 1 year. If Player 2 confesses and Player 1 refuse to disclose the crime, then Player 2 will go free, but Player 1 will undergo the 5 year punishment. According to Brams, disclose-disclose outcome is compromise, because it requires their best payoffs.[561] Also, Turocy and Stengel state that "*the defection from that mutually beneficial outcome is to confess, which gives a higher payoff no matter what the other does, with a resulting lower payoff to both. This constitutes their dilemma*."[562] The confession is the dominant strategy in the Prisoners' Dilemma and has a Nash Equilibrium.[563] The prisoners chose this because they had no communication, and could not trust each other to be able to choose to confess against each other.

The Prisoners' Dilemma applied to the arms race during the Cold War. It can also be applied to the problem of cooperation.[564] Prisoners' Dilemma shows us how Game Theory could be applied during the Cold War strategies of both sides. Along with other scholars[565], I will use Prisoners' Dilemma and apply it to the nuclear arms race.

[560] The numbers are chosen by randomly. Also first numbers belong to player 1 and second numbers belong to player 2.

[561] *Ibid*.

[562] Turocy and Stengel, *op.cit*., p. 10

[563] "Nash Equilibrium and Dominant Strategies", Available at: http://economics.fundamentalfinance.com/game-theory/nash-equilibrium.php (Accessed at: 01/09/2016)

[564] "Prisoners' Dilemma and the Problem of Cooperation", Available at: http://www.baselpeaceoffice.org/sites/default/files/imce/articles/News/nuclear_prisoners_dillemma.pdf (Accessed at: 01/09/2016); Turocy and Stengel, *op.cit.*

[565] For example, Colman, *op.cit*.; Plous, S. (1993), "The Nuclear Arms Race: Prisoners' Dilemma or Perceptual Dilemma?", *Journal of Peace Research*, Vol. 30 (2), Available at: http://www.jstor.org/stable/pdf/425197.pdf (Accessed at: 02/09/2016)

		Soviet Union	
		Not Build	**Build**
United States	**Not Build**	**(n, n) 3, 3**	**(n, b) 1, 4**
	Build	**(b, n) 4, 1**	**(b, b) 2, 2**

Table 9: The Prisoners' Dilemma Game and Nuclear Arms Race[566]

According to the table, if the US chooses not to build nuclear arms and the Soviet Union chooses not to build nuclear arms, the governments are not engaged in an arms race, but if the Soviet Union chooses to build nuclear arms, the Soviet Union gains a power advantage over the US. On the other hand, if the Soviet Union does not build, but the US does build, then the US gains a power advantage over the Soviet Union. But if both of them choose to build nuclear arms, then the two countries are engaged in an arms race. When we look at the preferred outcomes of the states, the US preferred outcome is ***bn,*** which is that the US builds nuclear weapons, but the Soviet Union does not. The second most preferred outcome for the US is the ***nn.*** The ***nn*** (do not build nuclear arms) is better than the ***bb,*** which is the building of nuclear arms by both states in an arms race, because the ***nn*** enables both states to save money, which they can spend on areas. The least preferred outcome for the US is ***nb.*** If the US chooses this strategy, the Soviet Union will gain power over the US, and the US will lose its position. Briefly, the US most preferred choices are **bn**>**nn**>**bb**>**nb.** On the other hand, the Soviet Union's preferred strategies are **nb**>**nn**>**bb**>**bn**. (here ***nb*** is the Soviet Union builds, but the US does not build, ***nn*** and ***bb*** is explained above, and lastly ***bn*** is the Soviet Union does not build, but, on the other hand, the US builds and gains a power advantage).[567]

As stated above, there is a dominant strategy in the Prisoners' Dilemma, the dominant strategy for both sides being to build nuclear arms, and the game produces the ***bb*** outcome for both sides. Although the ***nn*** outcome is better than the ***bb*** outcome**,** both states choose their dominant strategy to build nuclear arms, and this creates Nash equilibrium. This situation is explained by the Basel Peace Office as: "*The central factor preventing governments from realizing the gains available from mutual restraint in nuclear weapons programs is the lack of a mechanism with which to enforce agreements. If there existed a third party (the equivalent of a police force and the judiciary in domestic political systems) to enforce an*

[566] This table was retrieved from Colman's book. Colman, *op.cit.*, p. 118

[567] "Prisoners' Dilemma and the Problem of Cooperation", *op.cit.;* Plous, *op.cit.*

agreement, then it would be possible for the two countries to achieve the cooperative outcome. With an effective enforcement mechanism the US and the Soviet Union could agree to play ‘do not build’ strategies and, because cheating on this agreement would be punished, both would abide by the agreement. In the anarchic international system, however, no third party capable of enforcing agreements exists. Without an enforcement mechanism neither the United States nor the Soviet Union has an incentive to trust the other to abide by any agreement they make. Unwilling to risk facing their least preferred outcome in which they show restraint while the other country increases its nuclear power, both governments will play their dominant strategies. The anarchic nature of the international system, therefore, creates incentives for governments to engage in arms races, and makes it difficult for governments to bring these arms races to an end.”[568] It seems clear that the anarchic nature of the international arena creates difficulties for states to cooperate each other, and this situation also causes trust problems between states. The Prisoners’ Dilemma is important in terms of showing the weaknesses of the political institutions in the international system.[569]

3.4. Chicken Game

The Chicken game originated from the Hollywood movie, *Rebel Without a Cause*.[570] According to the Chicken game, there are two drivers, who drive their cars towards each other. There are two options for the players, to swerve or to drive straight.[571] If one of them swerves before another, this driver is called chicken. If both swerve together, no one is called chicken.

		Driver 2	
		Swerve	**Drive Straight**
	Swerve	**3, 3**	**1, 4**
Driver 1	**Drive Straight**	**4, 1**	**0, 0**

Table 10: The Chicken Game

[568] *Ibid.*
[569] *Ibid.*
[570] Poundstone, *op.cit.*, p. 197; Colman, *op.cit.*, p. 111
[571] Kolokoltsov, V. N. and Malafayev, O. A. (2010), *Understanding Game Theory: Introduction to the Analysis of Many Agent Systems with Competition and Cooperation*, London: World Scientific, p. 21

If both drivers swerve, the outcome is a draw, and their payoffs are 3-3, and if both drive straight ahead, they are at risk of death or injury, as payoffs 0-0. But if one driver chooses to swerve and the other driver chooses to drive straight ahead, the driver who chose to swerve has lost the game and is called chicken, although his or her payoff is 1, because there is no risk of death or serious injury.[572] There is a cooperative payoff in a swerve-swerve strategy[573], but it is not a dominant strategy for either, and therefore, this outcome cannot be explained as Nash equilibrium.[574] There are two Nash equilibria in the Chicken game,[575] being the Swerve-Drive Straight and the Drive Straight-Swerve. Also, there is a risk in playing this game, because when one of the drivers tries to maximize his or her payoff, they will have different outcomes if both choose to drive straight ahead. Colman evaluates the Chicken game as a dangerous game, and according to him, it has some peculiar properties. Colman explains these properties as: "*the first is its compulsive character: it is impossible to avoid playing with someone who is insistent. A person who has refused a challenge to play Chicken has effectively played and lost. The second peculiarity concerns the effects of commitment. A player who succeeds in making a credible commitment to choose the risky D strategy is bound to win at the expense of the other player, provided the other player is rational. This provides a game theory interpretation of the motto 'Who dares wins' of the dreaded British Special Air Service (SAS). A person who enjoys a reputation of recklessness is at a decided advantage in a game of Chicken on account of the fear that this induces in any rational opponent. A third peculiarity of Chicken revolves around what Daniel Ellsberg called 'the political uses of madness'. A player, who is seen to be irrational, not in control, or frankly 'crazy', gains a paradoxical advantage in a game of Chicken: people tend to give a wide berth to a lunatic*."[576] Although there are many risks in the Chicken game as detailed above, it has been used to model the Cuban Missile Crisis in 1962.[577]

The Cuban Missile Crisis was the most dangerous confrontation between the United States and the Soviet Union.[578] The Soviet Union installed medium-range and intermediate-range nuclear armed ballistic missiles in Cuba in October 1962, and these missiles had the capacity

[572] Colman, *Ibid*.; Zagare, F. C. (2014), "A Game-Theoretic History of the Cuban Missile Crisis", *Economies*, Vol. 2, Available at: http://www.mdpi.com/2227-7099/2/1/20 (Accessed at: 04/09/2016), p. 22

[573] Poundstone, *op.cit*., p. 199; Zagare, *Ibid*.

[574] Colman, *op.cit*., p. 112; Zagare, *Ibid*., p. 23

[575] Brams, S. J. (2003), *Negotiation Games: Applying Game Theory to Bargaining and Arbitration*, London: Routledge, p. 104

[576] Colman, *op.cit*., pp. 112-113

[577] Paravantis, J. A. (2016), "From Game Theory to Complexity, Emergence and Agent-Based Modeling in World Politics", in Tsihrintzis, G. A., Virvou, M. and Jain, L. C. (eds.) (2016), *Intelligent Computing Systems: Emerging Application Areas*, Berlin: Springer, p. 42

[578] Brams, *op.cit*., p. 104

to hit many parts of the United States.[579] The main aim of the United States was the removal of these missiles from Cuba, and it had two different strategies to protect its territory and power against the Soviet Union. These were the blockade or using air strikes to wipe out the installed missiles.[580] Table 11 shows the outcomes of the United States and the Soviet Union in the game of Chicken.

		Soviet Union	
		Withdraw	**Maintain**
United States	**Blockade**	**3, 3**	**1, 4**
	Air Strike	**4, 1**	**1, 1**

Table 11: Cuban Missile Crisis

It is clear from the table that the Soviet Union also had two different strategies against the United States strategies: withdrawal of the missiles or maintaining of the missiles. The best outcome or payoff for both sides was the 4 and the worst outcome 1 for each. If the United States chose to use a blockade and the Soviet Union responded to this strategy with a withdrawal of the missiles, then both sides' outcome would be 3 and the crisis have ended in compromise. But, if the United States chose to use air strikes, and the Soviet Union responded to this strategy by maintaining their missiles in Cuba, then the international community would be faced with nuclear war. On the other choices, if the United States chose air strikes and the Soviet Union chose withdrawal of the missiles, the crisis would end with a United States victory and outcome of 4, but, if the United States chose blockade, but the Soviet Union chose to maintain the missiles, then the crisis would end with a Soviet Union victory. According to Brams, "*the compromise (3, 3) outcome is not equilibrium because each player has an incentive to defect from it, and neither player has a dominant strategy; cooperation is best if the other player does not cooperate, but non-cooperation is best if the other player cooperates".*[581] The Nash equilibrium in the table is Air Strike-Withdraw (4, 1) and Blockade-Maintain (1, 4). Colman states that the Cuban Missile crisis ended with the Blockade-Withdraw strategies of both sides.[582] Brams explains why both sides chose to compromise: because there was no stable outcome without a blockade-withdraw strategy. As

[579] Brams, S. J. (2001), Game Theory and the Cuban Missile Crisis, Available at: https://plus.maths.org/content/game-theory-and-cuban-missile-crisis (Accessed at: 04/09/2016); *Ibid*., p. 105

[580] Brams (2003), *op.cit*., pp. 104-105

[581] Brams, S. J. (1985), *Rational Politics: Decisions, Games, and Strategy*, London: Academic Press Limited, p. 118

[582] Colman, *op.cit*., p. 114

explained above, there is no dominant strategy in the Chicken game, and each player's best strategy is based on the strategy of the other player. For example, if the United States chose blockade, the Soviet Union would have preferred withdrawal of the missiles, but if the United States chose air strikes, then the Soviet Union would have preferred maintaining the missiles.[583] The outcome was stable and neither of the players chose the worst outcome, which was the air strike-maintaining (1, 1).

3.5. The Application of Game Theory to Risks and Terrorism

Game Theory is generally applied by scholars to understand the Cold War era politics, some of which were detailed above. The above examples aimed to explain the application of Game Theory to threat perceptions such as the nuclear arms race and Cuban missile crisis, but following the Cold War, the understanding of threat perceptions has changed to risk and uncertainty. This can be clearly seen in the documents and strategic concepts of NATO. The new shift is different from the threat and the application of Game Theory to international politics in terms of risks can be problematic, but Cox states that risk analysis and Game Theory are complementary approaches.[584] Cox describes the application of Game Theory to risk analysis as: "*Game-theoretic analyses of conflicts require modelling the probable consequences of each choice of strategies by the players and assessing the expected utilities of these probable consequences. Decision and risk analysis methods are well suited to accomplish these tasks. Conversely, game-theoretic formulations of attack-defense conflicts (and other adversarial risks) can greatly improve upon some current risk analyses that attempt to model attacker decisions as random variables or uncertain attributes of targets ('threats') and that seek to elicit their values from the defender's own experts. Game Theory models that clarify the nature of the interacting decisions made by attackers and defenders and that distinguish clearly between strategic choices (decision nodes in a game tree) and random variables (chance nodes, not controlled by either attacker or defender) can produce more sensible and effective risk management recommendations for allocating defensive resources than current risk scoring models. Thus, risk analysis and game theory are (or should be) mutually reinforcing*."[585] As can be understood from this explanation, Game Theory is a useful tool to improve risk analysis in adversarial actions or in risk assessments. Also Bier *et al* state that Game Theory accounts for adversarial actions and can determine the

[583] Brams (1985), *op.cit*., pp. 121-122

[584] Cox, L. A. (2009), "Game Theory and Risk Analysis, *Risk Analysis*, Vol. 29 (8), Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01247.x/pdf (Accessed at: 10/09/2016), p. 1062

[585] *Ibid*.

probabilities of the consequences of different combinations in a game in terms of the actions of both sides, such as attacker and defender.[586] Bier *et al* clearly explain the application of Game Theory to risk as: "*certainly, game-theoretic models of attack and defense can provide useful concepts and computational tools for thinking about risks and allocating resources to defend infrastructure targets against intelligent attackers. The crucial insight from game theory, that rational players base their actions in part on what they expect others to do, is too important to ignore….To obtain realistic risk assessments and useful guidance for resource allocation, it is essential to take into account an adversary's possible adaptive behaviors, but without necessarily descending into the mathematical quagmire of full game theoretic modelling*."[587] As detailed earlier, both sides in Game Theory try to maximize their own payoffs, and therefore they do not care about the other side's thinking or doing. The Prisoners' Dilemma is the one of the most important examples to explain what the other side expects to do, and that one side must ignore the other side to improve its gain or payoff with a strategy. Bier *et al.* (above) show us that the attack-defence models of Game Theory provide the best way to explain risk assessment under the Game Theory. Cox also mentions that "*game-theoretic models and methods can help analysts think more clearly and effectively about the risks of adversarial situations by clarifying what should be modelled as decision variables for different players (i.e., the strategy sets of the players, which may include which targets to attack, under what conditions, when, and how) and what should be modelled as chance or consequence variables. These clarifications can make risk assessments more predictive and support more effective resource allocation decisions than decision and risk models that treat attacker decisions as random variables and that focus on eliciting and multiplying threat, vulnerability, and consequence estimates as if they were the means of random variables*."[588] When we look at risk assessment from the standpoint of Cox, it can be said that game-theoretic approaches' recommendations and predictions are more suitable than the Non-Game Theoretic approaches[589], because, as mentioned above, game theoretic analyses include what both sides expect in a game, or the conditions of both sides and their situations, and these conditions affect the strategy of both sides. Therefore game theoretic analysis of risk assessment gives better solutions and pathways than Non-Game Theoretic approaches.

[586] Bier, V. M., Cox, L. A. and Azaiez, M. N. (2009), "Why Both Game Theory and Reliability Theory Are Important in Defending Infrastructure Against Intelligent Attacks", in Bier, V. M. & Azaiez, M. N. (2009), *Game Theoretic Risk Analysis of Security Threats*, New York: Springer, p. 2

[587] *Ibid*., p. 3

[588] Cox, *op.cit.*, p. 1066

[589] *Ibid*.

Cox also indicates that special types of Game Theory models can be applied to terrorism risk analysis. According to him, leader-follower or attacker-defender games can give clear and simple analysis to aid terrorism risk analysis, the sequence of actions being as follows: 1. The defender tries to protect its resources from any attacks; 2. The attacker knows about the defender's actions for the protection of the various resources, and apportions resources to attacks the main targets; 3. Following both sides' strategies and choices, they reap the consequences of their actions.[590] Although Cox specifies the application of a special kind of Game Theory to terrorism, there are many alternative applications of Game Theory to terrorism.[591] According to Fuka *et al.*, Game Theory is a useful tool to research terrorism in several ways: "a*) captured terrorists and governments act interdependently; b) Government and the terrorists are rational actors who respond to opponents' steps; c) Government and terrorists behave so as to gain a strategic advantage; d) Government and terrorists are trying rationally to maximize their benefits; e) Government and terrorists make decisions on incomplete information".*[592] Sandler and Arce point to the ability of Game Theory to determine terrorists and targeted governments, states or international organisations as *".... six strengths of modern game theory for revealing quantifiable factors theoretically underlying the behaviour of terrorists and targeted governments: game theory (1) captures the interdependent nature of such interactions, (2) helps discover the strategic implications when each side acts according to its best guess about how the other side thinks, (3) incorporates the impact of threats and promises from each side, (4) takes advantage of the observation that 'players' tend to maximize goals subject to constraints, (5) helps predict outcomes in bargaining over demands, and (6) acknowledges the impact of uncertainty -incomplete*

[590] *Ibid*., pp. 1062-1063

[591] Sandler, T. and Siqueira, K. (2008), "Games and Terrorism: Recent Developments", *Simulation&Gaming*, Available at: http://www.utdallas.edu/~tms063000/website/Sandler_Siqueira_S&Gonline.pdf (Accessed at: 10/09/2016); Lapan, H. E. and Sandler, T. (1993), "Terrorism and Signalling", *European Journal of Political Economy*, Vol. 9, Available at: http://ac.els-cdn.com/017626809390006G/1-s2.0-017626809390006G-main.pdf?_tid=f8e4c702-8356-11e6-ba11-00000aacb361&acdnat=1474832204_197185a5e5e72c040eaab65155a4fd40 (Accessed at: 10/09/2016); Lee, D. R. (1988), "Free Riding and Paid Riding in the Fight Against Terrorism", *The American Economic Review*, Vol. 78 (2), Available at: https://www.jstor.org/stable/pdf/1818091.pdf (Accessed at: 10/09/2016); Sandler, T. and Arce, D. G. M. (2003), "Terrorism and Game Theory", *Simulation&Gaming*, Vol. 34 (3), Available at: http://www.utdallas.edu/~tms063000/website/Terror_Games.pdf (Accessed at 10/09/2016); Sandler, T. and Enders, W. (2002), *An Economic Perspective on Transnational Terrorism*, Available at: https://www.diw.de/sixcms/detail.php/39116 (Accessed at: 10/09/2016); Pate-Cornell, E. and Guikema, S. (2002), "Probabilistic Modelling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures", *Military Operations Research*, Vol. 7(4), Available at: http://onlinepubs.trb.org/onlinepubs/archive/conferences/mb/patecornellpaper.pdf (Accessed at: 10/09/2016)

[592] Fuka, J., Obrsalova, I. and Langasek, P. (2012), "Game Theory Application on Terrorism", *Advances in Economics, Risk Management, Political and Law Science*, Available at: http://www.wseas.us/e-library/conferences/2012/Zlin/EPRI/EPRI-37.pdf (Accessed at: 10/09/2016), p. 232

information- on all the above."[593] Sandler and Arce illustrate these six factors as "*an example of the shift away from skyjackings to kidnappings after the installation of metal detectors at airports in 1973 as evidence of a predictable and rational response to new constraints*."[594] On the other hand, Victoroff mentions the terrorist's expectations of success in his work as "*historical precedents*[595] *support many terrorists' expectations of success, so the theory of strategic choice must not be discounted on the grounds that terrorism's goals are uniformly improbable. Game-theoretical approaches are also sophisticated enough to recognize that the 'winnings' that satisfy terrorists may not be their overt anti-government goals but less obvious goals such as martyrdom, which may not only serve as an end in itself but also yield unexpected benefits to the terrorist's offspring that exceed the 'opportunity cost' of an educated life lost prematurely. Moreover, game theory has yielded evidence of counterintuitive but important predictions such as the possibility that government investments in deterrence might waste resources or even produce paradoxical increases in threat.*"[596]

According to the above information, states or international organisations may constitute their policies in accordance with the predictions of the officials and policy-makers, and lastly the level of terrorist/cyber terrorist attacks to targeted country or international organisations. According to Victoroff, "*Game Theory analysis is a powerful tool for discovering theoretically valid and surprisingly counterintuitive forces that probably influence terrorist and government behaviours. Game theory may also prove invaluable in predicting likely changes in the base rate (the rate predicted in rational actor simulations) of behaviours of an idealized terrorist in response to concessions or deterrent*."[597]

Sandler and Arce apply Game Theory to terrorism in terms of the proactive or reactive anti-terrorism policies of states. They used the Prisoners' Dilemma to explain these policies.

[593] Victoroff, J. (2005), "The Mind of the Terrorist: A Review and Critique of Psychological Approaches", *The Journal of Conflict Resolution*, Vol. 49 (1), Available at: https://www.surrey.ac.uk/politics/research/researchareasofstaff/isppsummeracademy/instructors%20/The%20Terrost%20mind.pdf (Accessed at: 03/10/2015), p. 14

[594] *Ibid*., pp.14-15

[595] Victoroff gives these examples for historical precedents, "*modern history is replete with examples of successful substate political violence: Irgun's bombings were a major factor in securing the independence of Eretz Israel from the British; terrorism by the Irish Republican Army (IRA) precipitated accommodations leading to the Irish Free State; Shi'ite Muslim terrorists provided key assistance in the ouster of the Shah of Iran; Hezbollah's suicide bombing campaign of 1983-1985 directly led to the American, French, and Israeli withdrawal and establishment of a Shi'a-controlled society in major parts of Lebanon; and the African National Congress (ANC) used terrorism as part of its remarkably successful strategy to overthrow the apartheid government of South Africa. More recently al Qaeda's brutal transnational campaign, including the mass murders at NewYork's World Trade Center in 2001, may have not only rapidly advanced Usama bin Laden's stated goal of removing the large U.S. military presence from Saudi Arabia but also served as an extremely potent recruiting tool.*" Victoroff, *Ibid*., p. 15

[596] *Ibid*.

[597] *Ibid*., p.16

		European Union	
		Pre-empt	**Do not pre-empt**
United States	**Pre-empt**	**2, 2**	**-2, 4**
	Do not pre-empt	**4, -2**	**0, 0**

Table 12: Prisoners' Dilemma and Terrorism

Sandler, T. and Arce, D. G. M. (2003), "Terrorism and Game Theory", *Simulation&Gaming*, Vol. 34 (3), Available at: http://www.utdallas.edu/~tms063000/website/Terror_Games.pdf (Accessed at 10/09/2016)

According to Sandler and Arce, "*proactive policy involves aggressively going after the terrorists and eliminating their resources, infrastructure, and personnel, while reactive policy concerns protective measures either to divert the attack or limit its consequences. A pre-emptive strike against the terrorists or their state sponsors (for example, the Taliban in Afghanistan) is an example of a proactive policy. Because a pre-emptive attack, if successful, eliminates the terrorist threat for all potential targets, there is a tendency to free ride or rely on the efforts of others.*"[598]

Sandler and Arce explain Table 12 as: the US and EU must decide to choose strategy between pre-empt or do not pre-empt. The pre-emption policy gives both sides 4 in benefits for both countries. If the US chooses pre-empt, but, on the other side, the EU does not pre-empt, then the US will have 4 benefits, but the EU loses its benefits to -2. This situation is reversed if the US chooses to not pre-empt, while the EU takes action to choose pre-empt. If both sides choose pre-emption, then each receives 2 in net benefits. According to Sandler and Arce, "*the resulting game is a Prisoners' Dilemma where no one takes an aggressive stance against the terrorists".*[599]

Another application of Game Theory to terrorism is the Cooperation Game, which includes assurance for both sides. Sandler and Arce again give an example of this game.

[598] Sandler and Arce, *op.cit.*, p. 7

[599] *Ibid.*, p. 8

		The UK	
		Retaliate	**Do Nothing**
	Retaliate	**4, 4**	**1, 3**
The US	**Do Nothing**	**3, 1**	**2, 2**

Table 13: Ordinal game Matrix for Retaliation

Sandler, T. and Arce, D. G. M. (2003), "Terrorism and Game Theory", *Simulation&Gaming*, Vol. 34 (3), Available at: http://www.utdallas.edu/~tms063000/website/Terror_Games.pdf (Accessed at 10/09/2016)

As is clear from Table 13, the best payoffs for both sides in the retaliation and second best payoffs come from doing nothing against terrorists. The worst payoffs are for both sides to choose, one side to retaliate and the other side to do nothing. The games have two different Nash equilibria in the retaliation-retaliation and do nothing for both sides.[600]

There are some differences between the Prisoners' Dilemma and Assurance Game here. Firstly, Prisoners' Dilemma has a dominant strategy and gives higher payoffs to each side's action, but in the Assurance Game there is no dominant strategy, and it does not give higher payoffs according to what the other side does. The second difference is that, with the improvement of terrorism threats, the coalition will give higher payoff to each side, while Prisoners' Dilemma includes selfishness and freeloading, which give higher payoff to each side. Therefore this is the dominant strategy for both sides in Prisoners' Dilemma. In the Assurance Game, if both sides trust each other and keep their word, they will have higher payoffs. The Prisoners' Dilemma encourages both sides towards selfishness, but the Assurance Game accelerates both sides towards coalition.[601] In accordance with this explanation, the US and the UK choose to retaliate against terrorism to have a higher payoff.

As mentioned above, there are other applications of game-theoretic model to terrorism, and it is not possible to give and analyse all of them here. The application of Game Theory to cyber terrorism has similar elements in terms of the higher payoffs. This will be explained in the next section.

3.6. The Application of Game Theory to Cyber Security

The details of Game Theory have been outlined in the previous sections. Game Theory is normally used in economics, but during the past decade, the theory has also been applied to

[600] *Ibid*., p. 17

[601] Özdamar, Ö. (2007), "Oyun Kuramının Uluslararası İlişkiler Yazınına Katkıları", *Uluslararası İlişkiler*, Vol. 4 (15), pp. 48-49

explain international relations. In the previous section, the application of Game Theory to terrorism was explained in detail, using examples.

With the changing nature of threat to risk, states and international organisations have tried to improve their critical infrastructures with new security policies. Bier *et al.* point out that states have many critical infrastructures[602] and are potentially vulnerable to any attacks committed by terrorists.[603]

Alpcan and Başar strongly mention in their work the importance of networked computing and communication systems and the defence of critical infrastructure in modern society.[604] They maintain: "*a good illustration of this fact is provided by the Internet, the epitome of networks that has evolved to a global virtual environment and become an indispensable part of our lives. Nowadays our communication, commerce, and entertainment are all based on networked systems in one way or another. Once they are disrupted its cost to society is hard to measure, but enormous, for sure*."[605] The Estonian example was detailed in Chapter 1 shows the importance of the protection of critical infrastructures, and according to Bier et al., researchers and scholars have tried to find new ways of dealing with this problem.[606]

Scholars have applied Game Theory to cyber security[607], the main aim of the application of Game Theory being to improve network and cyber security.[608] Alpcan and Başar mention that "*game theory provides a rich set of tools to study problems where multiple players with different objectives interact and compete with each other on the same system. Therefore, Game theory is a strong candidate to provide the much needed mathematical framework for analysis, modelling, decision, and control processes for information security and intrusion*

[602] Bier *et al.* give some examples to critical infrastructure as: oil and natural gas pipelines, electric power grids, transportation routes and facilities, telecommunications networks, water supply, built infrastructures, and food-production, processing, and distribution supply chains or networks information infrastructures. Bier *et al.*, *op.cit.*, p. 1

[603] *Ibid.*

[604] Alpcan, T. and Başar, T. (2011), *Network Security: A Decision and Game-Theoretic Approach*, Cambridge: Cambridge University Press, p. 4

[605] *Ibid.*

[606] *Ibid.*

[607] Roy *et al.*, *op.cit.*; Lye, K.W. and Wing, J. M. (2005), "Game Strategies in Network Security", *International Journal of Information Security*, Available at: http://www.cs.cmu.edu/~wing/publications/LyeWing05.pdf (Accessed at: 07/09/2016); Becker, S., Seibert, J., Zage, D., Nita-Rotaru, C. and State, R. (2011), *Applying Game Theory to Analyze Attacks and Defenses in Virtual Coordinate Systems*, Available at: http://ds2.cs.purdue.edu/papers/dsn2011_gametheory.pdf (Accessed at: 07/09/2016); Manshaei, M. H., Zhu, Q., Alpcan, T., Başar, T., and Hubaux, J. P. (2010), "Game Theory Meets Network Security and Privacy", *EPFL Technical Report*, Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.187.9377&rep=rep1&type=pdf (Accessed at: 07/09/2016)

[608] Liang, X. and Xiao, Y. (2013), "Game Theory for Network Security", *IEEE Communications Surveys&Tutorials*, Vol. 15 (1), Available at: http://yangxiao.cs.ua.edu/IEEE_COMST_game_2013.pdf (Accessed at: 07/09/2016)

detection”.[609] According to this view, it can be said that Game Theory is capable of analysing different possibilities, including each side’s expectations and psychological situations in determining the best action against each other in a game.[610]

As explained in previous sections, the Game theoretic approach requires at least two players[611], and the number of players can increase. The application of Game Theory involves four different components including players, strategic actions for each player, the payoff of each player and information structures in the game.[612] The main aim of both sides in the real game is to maximize their gains, and therefore different techniques are available in Game Theory.[613] According to Ibidunmoye, Alese and Ogundele, “*The benefit of quantifying network security using game-theoretic approach is enormous. Most importantly it may help network administrator to find the optimal defence strategies of a system and to calculate the expected loss associated with different defence strategies*.”[614] Liang and Xiao explain the application of Game Theory to network security as: “*Network security measurements involve the interactions of attackers and defenders, and the result of a measurement can be affected by their interactions. For example, one of the metrics in risk assessment for a network system is the probability of it being attacked. There is a need to predict the actions of both the defenders and the attackers. Since the interaction process between attackers and defenders is a game process, game theory can be applied in every possible scenario to predict the actions of the attackers and then to determine the decisions of the defenders. Therefore, game theory-based solutions have been proposed for network security problems*.”[615] It seems clear that the interactions between defenders and attackers affect security policies, and Game Theory helps the defenders to optimize their policies and develop optimal defence strategies against cyber-attackers.[616]

[609] Alpcan, T. and Başar, T. (2006), *An Intrusion Detection Game With Limited Observations,* Available at: http://www.tansu.alpcan.org/papers/isdg06.pdf (Accessed at: 08/09/2016), p. 1; Alpcan, T. and Başar, T. (2005), *A Game Theoretic Analysis of Intrusion Detection in Access Control Systems*, Available at: http://people.virginia.edu/~sdp5f/sys793/presentations/2005/07%20Henry%201012/Papers/alpcan-basar-cdc04_WeA05_6.pdf (Accessed at: 08/09/2016), p. 1

[610] Liang and Xiao, *op.cit.*, p. 472

[611] Roy, *et al., op.cit.,* p. 3

[612] *Ibid*., p. 14

[613] Hamilton, S. N., Miller, W. L., Ott, A. and Saydjari, O. S. (2002), “The Role of Game Theory in Information Warfare”, *Proceedings of the 4th Information Survivability Workshop*, Available at: https://verify.iaik.tugraz.at/research/pub/Ausgewaehltekapitel/WebHome2009/GT_in_IW.pdf (Accessed at: 10/09/2016), p. 1; Roy, *et al., op.cit.,* p. 3

[614] Ibidunmoye, E. O., Alese, B. K. and Ogundele, O. S. (2013), “Modelling Attacker-Defender Interaction as a Zero-Sum Stochastic Game”, *Journal of Computer Sciences and Applications*, Vol. 1(2), Available at: http://pubs.sciepub.com/jcsa/1/2/3/ (Accessed at: 10/09/2016), p. 27

[615] Liang and Xiao, *op.cit.*, p. 472

[616] Sungwook, K. (2014), *Game Theory Applications in Network Design*, Hershey: IGI Global, p. 165

Cyber security policies can be evaluated under the Non-Cooperative Games.[617] Stackelberg Games have been used by scholars to explain security problems, as this game models the interaction between a defender an attacker.[618]

Stackelberg games like other types of the Game theory have two players, and these players are called as a leader and follower.[619] In Stackelberg games the leader, or the defender, plays its strategy first and then a follower, or the attacker, optimizes his reward in accordance with the action chosen by the leader.[620] It can be understood from that each player has some possible strategies like the other versions of Game theory, but the different point of Stackelberg game according to An *et al.* is that *a "mixed strategy allows a player to play a probability distribution over pure strategies".*[621]

[617] Javidi, M. M. and Aliahmadipour, L. (2015), "Game Theory approaches in Taxonomy of Intrusion Detection for MANETs", *Computer Engineering and Applications*, Vol. 4 (1); Roy *et al., op.cit*., p. 4

[618] Jain, M., An, B. and Tambe, M. (2013), "Security Games Applied to Real-World: Research Contributions and Challenges", in Jajodia, S., Ghosh, A. K., Subrahmanian, V. S., Swarup, V., Wang, C. and Wang, X. S. (2013), *Moving Target Defense II: Application of Game Theory and Adversarial Modelling*, London: Springer, p. 16; von Stengel, B. and Zamir, S. (2004), "Leadership with Commitment to Mixed Strategies", *CDAM Research Report*, Available at: http://www.cdam.lse.ac.uk/Reports/Files/cdam-2004-01.pdf (Accessed at: 11/09/2016), p. 2; An, B., Tambe, M., Ordonez, F., Shieh, E. and Kiekintveld, C. (2011), "Refinement of Strong Stackelberg Equilibria in Security Games", *Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence*, Available at: http://teamcore.usc.edu/people/boa/papers/bo-an_aaai11.pdf (Accessed at: 11/06/2016), p. 587; Jain, M., Kardeş, E. and Ordonez, F. (2010), "Security Games with Arbitrary Schedules: A Branch and Price Approach", *Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence*, Available at: http://teamcore.usc.edu/manish/files/aaai10.pdf (Accessed at: 11/06/2016), p.1; Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordonez, F. and Tambe, M. (2009), "Computing Optimal Randomized Resource Allocations for Massive Security Games", *8th International Conference on Autonomous Agents and Multiagent Systems*, Available at: http://delivery.acm.org/10.1145/1560000/1558108/p689-kiekintveld.pdf?ip=85.99.163.111&id=1558108&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2EA13CBF7F1C3C7DF4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=678714832&CFTOKEN=92564710&__acm__=1475925958_4cdcf7992682e234cfbb37f986c7af1d (Accessed at: 11/06/2016), p. 690; Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., and Tambe, M. (2011), "Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness", *Journal of Artificial Intelligence Research*, Vol. 41, Available at: http://www.aaai.org/Papers/JAIR/Vol41/JAIR4109.pdf (Accessed at: 11/06/2016), p. 297

[619] Korzhyk *et al., op.cit*., p. 297; Paruchuri, P., Pearce, J. P. and Kraus, S. (2008), "Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games", *AAMAS 08 Proceedings of the 7the International Joint Conference on Autonomous Agents and Multiagent Systems*, Available at: http://delivery.acm.org/10.1145/1410000/1402348/p895-paruchuri.pdf?ip=85.99.163.111&id=1402348&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2EA13CBF7F1C3C7DF4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=678714832&CFTOKEN=92564710&__acm__=1475925923_a1bb56565bf63e4fd876128226ff6692 (Accessed at: 12/09/2016), p. 895; Pita, J., Jain, M., Tambe, M., Ordonez, F. and Kraus, S. (2010), "Robust Solutions to Stackelberg Games: Addressing Bounded Rationality and Limited Observations in Human Cognition", *Artificial Intelligence*, Vol. 174, Available at: http://teamcore.usc.edu/papers/2010/AIJ3.pdf (Accessed at: 12/09/2016), p. 5

[620] An, B., Tambe, M. and Sinha, A. (2015), "Stackelberg Security Games (SSG) Basics and Application Overview", *Nanyang Technological University*, Available at: http://www.ntu.edu.sg/home/boan/papers/Milindchapter.pdf (Accessed at: 12/09/2016), p. 3

[621] *Ibid*.

	c	**d**
a	**2, 1**	**4, 0**
b	**1, 0**	**3, 2**

Table 14: Payoff Table for Example Stackelberg Game

The table illustrates the advantages of being the leader in a Stackelberg game.[622] The leader is the row player, with strategies *a* and *b*, and the follower is the column player, with strategies *c* and *d*. There is only one Nash equilibrium in this game, when the leader plays *a* and the follower chooses *c*, which gives the leader a payoff of 2.[623] On the other hand, strategy *b* is the strictly dominant strategy for the leader.[624] If the leader chooses to play strategy *b* before the follower chooses his/her strategy, then the leader will have a higher payoff of 3; the follower then chooses to play strategy *d* to obtain higher payoff for him/herself. The main difference of Stackelberg game from the other versions of Game Theory is that if the leader wants to commit a mixed strategy of playing *a* and *b* equal as 0.5 probability, then the follower will choose to play strategy *d* to have higher payoff for himself and the other side, and the leader's expected payoff will be 3.5.[625]

An *et al.* state that Stackelberg game can be used in security, with the leader being modelled as a security force and the attacker modelled as a terrorist.[626] They also mention that "*the defender commits to a mixed (randomized) strategy, whereas the attacker conducts surveillance of these mixed strategies and responds with a pure strategy of an attack on a target. Thus, the Stackelberg game framework is a natural approximation of the real-world security scenarios*."[627] According to Brown *et al.*, "*the key assumptions that make a Stackelberg game appropriate for security (1) the attacker's and defender's actions are sequential, (2) the attacker has a perfect model of how the defender will (or should) optimally operate the system, even after an attack, and (3) the attacker will manipulate that system to his best advantage. The latter two assumptions are strong but prudent for us: The defender can suffer no worse should the attacker possess a less-than-perfect model of the defender's*

[622] *Ibid.*

[623] Paruchuri, P., Pearce, J. P., Marecki, J., Tambe, M., Ordonez, F., and Kraus, S. (2008), "Efficient Algorithms to Solve Bayesian Stackelberg Games for Security Applications", P*roceedings of the Twenty-Third AAAI Conference on Artificial Intelligence*, Available at: https://www.aaai.org/Papers/AAAI/2008/AAAI08-262.pdf (Accessed at: 12/09/2016), p. 1559

[624] *Ibid.*

[625] *Ibid.*

[626] *Ibid.*, p. 4

[627] *Ibid.*

system, or fail to implement a perfect attack plan.”[628] Tambe gives an example of Stackelberg Security Game in his work. According to him, there is an airport with two terminals, Terminal 1 and Terminal 2, but there is only one police unit to protect the terminals from any attacks by one attacker.[629] Tambe evaluates Terminal 1 as being more important than Terminal 2.

		Attacker	
		Terminal 1	**Terminal 2**
Defender	**Terminal 1**	**5, -3**	**-1, 1**
	Terminal 2	**-5, 5**	**2, -1**

Table 15: Stackelberg Security Game

Tambe, M. (2012), *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*, Cambridge: Cambridge University Press, p. 4

Table 15 shows that the defender has two options, in terms of protecting Terminal 1 or Terminal 2, and, on the other side, the attacker has two options of attacking Terminal 1 or Terminal 2. As mentioned above, Terminal 1 is more important than Terminal 2 and therefore the police will always seek to protect Terminal 1 from any attack. If the attacker knows about the aim of the defender to always protect Terminal 1, then the attacker will attack Terminal 2. If the attacker succeeds in the attack, then the attacker will have a payoff of 1, and the police will have a payoff of -1. This situation will reverse if the police protect Terminal 2 and the attacker attacks Terminal 1, as the payoffs are -5 and 5. But, on the other hand, if the attackers attack any Terminal which the police protect, then the attacker will be captured and the police will have more payoffs than the attacker.[630]

According to Tambe, if the police changed their strategy to protect both Terminals at different hours of the day, such as spending 60% of their time in Terminal 1 and 40% in Terminal 2, then the police would have a better result against the attacker, because the attacker would not know where the police will be tomorrow.[631] This situation increases the

[628] Brown, G., Carlyle, M., Salmeron, J. and Wood, K. (2006), “Defending Critical Infrastructure”, *Interfaces*, Vol. 36 (6), Available at: http://calhoun.nps.edu/bitstream/handle/10945/36732/defending_critical_infrastructure.pdf?sequence=1 (Accessed at: 12/09/2016), p. 532

[629] Tambe, M. and Jain, M. (2012), “Introduction and Overview of Security Games”, in Tambe, M. (2012), *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*, Cambridge: Cambridge University Press, p. 4

[630] *Ibid*.

[631] *Ibid*., p. 6

uncertainty for the attacker and improves the payoff for the police.[632] This randomized strategy is known as a mixed strategy.[633]

Jain *et al.* explain the solution of security games with mixed strategy, where the defender maximizes the expected utility, and on the other side, the attacker knows the mixed strategy of the defender and plays best-response for himself[634], and "*this solution is accepted as Stackelberg equilibrium which assumes that the follower will always break ties in favour of the leader in cases of indifference. This is because a Strong Stackelberg equilibrium (SSE) exists in all Stackelberg games, and additionally, the leader can always induce the favourable strong equilibrium by selecting a strategy arbitrarily close to the equilibrium that causes the follower to strictly prefer the desired strategy.*"[635]

Jain *et al.* further define SSE as:

> *"A pair of strategies from a Strong Stackelberg Equilibrium (SSE) if they satisfy:*
>
> 1) *The defender plays a best-response, that is, the defender cannot get a higher payoff by choosing any other strategy.*
> 2) *The attacker plays a best-response, that is, given the defender's strategy, the attacker cannot get a higher payoff by attacking any other target.*
> 3) *The attacker breaks ties in favour of the leader".*[636]

As detailed above, Stackelberg Security Games have been used to analyse real situations. For instance, at Los Angeles International Airport, where ARMOR was deployed at randomized checkpoints.[637]

In the next section, I will evaluate the Estonian case under the Game Theory. The application of Game Theory to the Estonian cyber-attack will be the first implementation of the case study. There is only one work on the application of Prisoner's Dilemma to Estonia, but this research does not justify or analyse the cyber-attacks/cyber security policies: it only evaluates

[632] *Ibid.*
[633] *Ibid.*
[634] Jain *et.al.* (2013), *op.cit.*, p. 18
[635] *Ibid.*
[636] *Ibid.*, p. 19
[637] See for more information; An, *et.al* (2015), *op.cit.*; Pita, J., Jain, M., Ordonez, F., Portway, C., Tambe,M., Western, C., Paruchuri, P. and Kraus, S. (2009), "Using Game Theory for Los Angeles Airport Security", *Al Magazine*, Available at: https://u.cs.biu.ac.il/~sarit/data/articles/AI_Magazine09.pdf (Accessed at: 13/09/2016); Pita, J., Jain, M., Ordonez, F., Portway, C., Tambe,M., Western, C., Paruchuri, P. and Kraus, S. (2008), "Deployed ARMOR Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport", *AAMAS '08 Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems: Industrial Track,* Available at: http://teamcore.usc.edu/papers/2008/AAMASind2008Final.pdf (Accessed at: 13/09/2016)

the relationship between Russia and Estonia under the Powerful Nation v. Less-Powerful Nation during the Estonian cyber-attacks.[638]

3.7. Assessing the Estonian Attack Using Game Theory

Although Estonia was advanced in its use of the Internet and communication systems,[639] their lack of security systems, and vulnerability against cyber-attack made it easy for a series of cyber-attacks to succeed.[640]

We start from the premise that, given the nature of the threat, we might expect countries to provide significant resources towards combatting the threat of cyber-attacks. Proper resourcing could result in little to no loss, and high profits (payoff), such as protection of infrastructure, and determining the attackers, but as Estonia (and other examples) illustrates, countries have traditionally sought to pay as little as possible in order to protect themselves. In addition, state activities have to operate within the international law, so individual states and international organisations have limitations. If we contrast the position of the terrorist/attacker, who only pays their computer and internet fees and have no limits in terms of laws, procedures and bureaucracy, it seems axiomatic that states should give more attention and provide more resources for protection against this type of attack, resulting in more payoff than the terrorists and attackers.

States and international organisations generate their security policies according to risk assessment and threat perceptions. Also geographical, economic and political situations tend to affect states' security policies. The international community has been trying to solve the problem of terrorism, and many states have adopted new security policies to protect their citizens from any terrorist attack. If we think about the security policies in terms of Stackelberg security game, states have limited resources and yet must protect themselves against unlimited threats, risks and uncertainty.

[638] Kostyuk, N. (2013), "The Digital Prisoner's Dilemma: Challenges and Opportunities for Cooperation", *World Cyberspace Cooperation Summit IV*, Available at: http://cybersummit.info/sites/cybersummit.info/files/The%20Digital%20Prisoner's%20Dilemma-Challenges%20and%20Opportunities%20for%20Cooperation_Nadiya%20Kostyuk%20.pdf (Accessed at: 12/09/2016)

[639] Such as Turkey and other 3rd World Countries.

[640] Richards, *op.cit.*

		Terrorists	
		Counter-Terrorism	**Cyber-Terrorism**
Estonia	**Counter-Terrorism Policy**	**4, -2**	**-2, 2**
	Cyber-Terrorism Policy	**-2, 2**	**3, -1**

Table 16: Stackelberg Security Game for Estonia Cyber-attacks

The table illustrates the cyber-attacks on Estonia under the Stackelberg Security Game. As detailed in Chapter 1, Estonia faced a series of cyber-attacks in 2007, and the country did not use its cyber infrastructure effectively during these attacks. Estonian officials state that although Estonia has used internet sources more effectively in all areas, they have not improved the cyber infrastructure against any attacks. The table shows that if Estonia only adopts a counter-terrorism policy, and terrorists attack via information technology, then Estonia will have payoff of -2, while on the other side, the terrorists will have payoff of 3. This situation reverses when Estonia adopts a cyber-terrorism policy.

As stated in Chapter 1, Estonia did not improve its cyber security against any cyber-attack, and this situation was used by cyber-terrorists to attack critical governmental places to succeed in their aims. If this case is evaluated under the Stackelberg game, the cyber-terrorists will have more payoff than Estonia, and the cyber-terrorists’ attack succeeds. It may be understood that, prior to the 2007 attacks Estonia had paid little or no attention to its cyber security policies, therefore, the cyber terrorists had more payoffs than Estonia.

This situation, however, has now changed, with Estonia paying much more attention to cyber security, eventually leading to the state having more of a payoff than the cyber-terrorists, and thereby providing greater protection from future attacks. Using this simple example to evaluate the cyber terrorist attacks on Estonia under the fractions of Stackelberg security game, Estonia has chosen to play mixed strategies against terrorists. As mentioned previously, the leader or defender has the right to play first, and choose best-response against cyber-terrorists. After the chosen strategy by the defender, Estonia, the attacker must play a best-response in accordance with the defender strategy, and the attacker cannot have a higher payoff by attacking any other target. The chosen strategy by the attacker breaks the tie, and the leader will have more payoff than the attacker. This situation is known as a Strong Stackelberg Equilibrium.

To sum up, Game Theory and its fractions help states to determine their payoffs and pay-outs against cyber-terrorists. It is clear that states and international organisations must improve their securities against any attacks, and that if they leave empty any sources or critical infrastructures, they will lose their position against attackers.

3.8. Conclusion

The popularity of the application of Game Theory to international politics has increased during past decades. The theory had normally been applied to economics and mathematics, but during the Cold War, the theory was applied to Cold War term threats, such as the Cuban Missile Crisis and Nuclear Arms race. The application of Game Theory to Cold War term dynamics in terms of international relations and politics was easy, because there were only two different sides and threats in the international community. Since the collapse of the Soviet Union, the international community has faced different threat perceptions, risks and uncertainties, and this situation has created different problems for the international community. New security policies have been implemented to protect international peace and security from the new threats, risks and uncertainties. Although the calculation of the Cold War term dynamics was easy in terms of Game theoretical approach, scholars are used to applying Game Theory to analyse the new term dynamics. The fractions of Game Theory help scholars and academics to analyse and calculate expected payoffs and the security policies for the states and international organisations. As mentioned in previous sections, Game Theory has been used to analyse terrorism under the cooperation, retaliation, and Prisoner's Dilemma. Also, Stackelberg games have been successfully used by states to protect important places such as Los Angeles Airport.[641] Game Theory has an important role in improving security policies against new threats, risks and uncertainties. The successful application of Game Theory was seen in the Cold War era, and the theory has continued to pursue this achievement since the Cold War in terms of the application of risks and terrorism threats. Game Theory can be applied to cyber threats and cyber-terrorism issues in order to solve security problems for both states and international organisations. States and international organisations can use it to calculate their payoffs against any cyber-attacks, in line with their security policies.

The theory has been chosen by researcher to calculate the expected payoff structure for states and international organisations. If states and international organisations expend more effort

[641] See Footnote 124

on other threats and risks, then they will face the threat of cyber-attacks, and they will lose their position against attackers. The Stackelberg Security games have shown the importance of mixed strategies and policies against attackers and terrorists.

CHAPTER 4: THE APPLICATION OF INTERNATIONAL LAW

4.1. The Development of International Law

It is not possible to explain or discuss all the developments in international law here, but the aim of this chapter is to identify those developments that have significance for this thesis and provide a little historical background.

International law has a long history. There have been many treaties between states, such as the treaty between Lagash and Lumma in 2454-2455 BC[642] and an Egyptian and Hittite peace treaty from around 1259 BC.[643] With the foundation of modern states, the concept of sovereignty emerged. Writing in 1576 Bodin said that, sovereignty could not be granted by law; it was subject to the laws of God and of nature.[644] Natural law theory can trace its origins to the middle ages where the Catholic Church was a major influence on international relations and law.[645] For example Shaw quotes from Saint Thomas Aquinas book, Summa Theologia:

> "*Reason, declared Aquinas, was the essence of man and thus must be involved in the ordering of life according to the divine will. Natural Law was the fount of moral behaviour as well as of social and political institutions, and it led to a theory of conditional acceptance of authority with unjust laws being unacceptable*."[646]

Important developments in international law came after the 17th Century. Significantly in *On the Law of War and Peace (De Jure Belli Ac Pacis)* Hugo Grotius (often referred to as the 'father of international law') sought to exclude theology from international law.[647] According to him, "*the law of the nature would be the same, if God did not exist.*"[648] Significantly he identifies the law of nations as a distinct source of law, rather than simply the law of nature: "*the law of nations was the law which has received its obligatory force from the will of all*

[642] King, L., *Eannatum of Lagash 2454-2455 BC*, Available at: http://www.cristoraul.com/ENGLISH/readinghall/GalleryofHistory/Ancient-People/EANNATUM.html (Accessed at: 22/08/2012). Kramer, S. N. (1963), *The Sumerians; Their History, Culture and Character*, Chicago: University of Chicago Press, pp.56-57

[643] Bryce, T. (2006), "The "Eternal Treaty" from the Hittite Perspective, *BMSAES*, Vol. 6, Available at: http://www.britishmuseum.org/pdf/6a%20The%20Eternal%20Treaty.pdf (Accessed at: 22/08/2012), pp. 1-11

[644] Shaw, M. (2008), *International Law*, Cambridge: Cambridge University Press, p.21

[645] Neff, S. C. (2010), "A Short History of International Law", in Evans, M. (ed.) (2010), *International Law*, Oxford: Oxford University Press, p.34

[646] Shaw, *op.cit.*, p. 22

[647] Neff, *op.cit.*, p.37, Shaw, *Ibid.*, p.24

[648] Neff, *Ibid.*, Shaw., *Ibid.*

nations or of many nations."[649] He believed that the law of nature could be improved, but needed the power of the state for protection, and for the state to act as guarantor of the law. After Grotius, debate on the theoretical underpinning of international law continued to develop, including the distinctions between the law of nature and nations. In *The Law of Nature and Nations,* Samuel Pufendorf sought to link international law with the law of nature. For Thomas Hobbes the law of nature was to be found in the nature of men and the nature of rights:

> *"a precept, or general rule, found out by reason, by which a man is forbidden to do that which is destructive of his life, or takes away the means of preserving the same; and to omit that by which he thinks it may best be preserved."*[650]

Nevertheless, agreements, treaties and customs were accepted and recognised by states as essential elements of the law of nations.[651] With the developments of new ideas in international relations and law following the Peace of Westphalia in 1648[652], positivism emerged as an influential theory.[653]According to August Comte writing in 1830,[654] the theory of positivism was about true knowledge, which was only that which could be verified scientifically. This does not include theology or metaphysical knowledge from nature.[655] Comte identified three stages in the development of the human race: theological, metaphysical and positive.[656] The theological stage was controlled by the power of religions, such as the Catholic Church. People used the doctrine of the Church rather than their own rational choices.[657] Logical, legalistic and natural laws were used in the metaphysical stage.[658] The last stage of the human race is the positivist one which is based on scientific and individual rights being more important than other rules.[659] According to Comte, all stages have to be completed to find truth. Neff makes a helpful point for the purposes of this research:

[649] Neff, *Ibid*., p.37

[650] Hobbes, T. (1651), *op.cit*. p. 90

[651] Shaw, *op.cit*., p.26

[652] "The Peace of Westphalia was not one specific treaty but rather a collection of treaties commonly linked by the fact that they brought the Thirty Years War to an end." Trueman, C. N. (2015), *The Peace of Westphalia*, Available at: http://www.historylearningsite.co.uk/the-thirty-years-war/the-peace-of-westphalia/ (Accessed at: 06/01/2016)

[653] Shaw, *op.cit*.,p.26

[654] Neff, *op.cit*., p.41

[655] Larrain, J. (1979), *The Concept of Ideology*, London: Hutchinson Education, p. 197

[656] Neff, *op.cit*., p.41. Giddens, A. (1974), *Positivism and Sociology*, Aldershot: Ashgate Publishing Limited, p.1

[657] Mill, J. S. (2003), *Auguste Comte and Positivism*, London: Kessinger Publishing, p. 3.Neff, *op.cit*., p.41

[658] Neff, *Ibid.* Mises, R. V. (1951), *Positivism; A Study in Human Understanding*, Cambridge: Harvard University Press, p.5

[659] Neff, *op.cit*., p.41

> *"Perhaps the principal manifestation of positivism was the belief that law is entirely a human institution. In the realm of international law specifically, this meant that positivism was the clear heir to the voluntary law of the seventeenth and eighteenth centuries."*[660]

With the development of the positivist theory, the law of nature became less significant, and by the start of the 18th Century, positivism was considered more important than natural law in the field of international law. For example, Carlos Calvo who was the Argentinian international lawyer, declares the turn to positivism.[661] According to Lorca, "*the continuing purchase of naturalist doctrines constituted a threat to the independence of non-European states even Western governments had recognized their legal personality. Under natural law's argumentative plasticity, just war theory could justify Western military intervention in China, Turkey or Latin America. Semi-peripheral jurists thus realized the need to develop a comprehensive critique of natural law on 'scientific' grounds. Carlos Calvo, for example, did not simply join the positivist trend, but also described the distinction between natural law and positive law and the corresponding differentiation between customary law and conventional law as outdated….Calvo shifted the attention toward elucidating the principles of justice on the basis of which international law is founded and that ought to precede interstate relations. After reviewing the positions of a long list of authorities, Calvo summarizes his opinion: '[W]e recognize that the general idea of justice can transform the relations of states for the better and in their common benefit; however, in the course of our work we will stick with preference to the principles defined in treaties, to the rules naturally and logically deduced from particular conventions, or from the diverse cases resolved in practice, in short to the established jurisprudence.*"[662]

Whilst the 18th Century produced theories on international law, the 19th Century provided for a new international law system to be applied to some specific situations. For example following the Congress of Vienna, a new system emerged in Europe as a means of balancing power. According to Shaw:

> *"Over a century later the Napoleonic wars terminated with the Congress of Vienna in 1815, marking the first systematic attempt to regulate international affairs by means of regular international conferences. The Congress system lasted, in various guises, for practically a century and*

[660] Neff, *op.cit.*, pp.41-42

[661] Lorca, A. B. (2014), *Mestizo International Law: A Global Intellectual History 1842-1933,* Cambridge: Cambridge University Press, p. 58

[662] *Ibid.*, p.59

> *institutionalised not only the balance of power approach to politics, but also a semi-formal international order.'*[663]

Following these conflicts, the international community tried to create a new order, and started to provide new international law, together with international and regional organisations throughout the world. The International Telegraphic Union was established in 1865 and the Universal Postal Union in 1874.[664]

Following the First World War the first international organisation was established, the League of Nations.[665] The period of the League of Nations saw international law and organisational structures develop in terms of the founding of new institutions. The Permanent Court of International Justice was established in 1921 as a standing body at The Hague, but it was officially known after the Second World War as the International Court of Justice.[666]

Following the Second World War new regional organisations were established, such as NATO and the European Union (the EU). International law developed with new conventions, customs and treaties being agreed.

Together with the development of international relations and law, the sources of international law needed to be established. Article 38 (1) of the Statute of the International Court of Justice describes the sources of international law:

> *"the Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: (a) international conventions, whether general or particular, establishing rules expressly recognised by the contesting states; (b) international custom, as evidence of a general practice accepted as law; (c) the general principles of law recognised by civilised nations; (d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.'*[667]

[663] Shaw, *op.cit.*, pp.1282-83

[664] Akande, D. (2010), "International Organisations" in Evans, M. (ed.) (2010), *International Law,* Oxford: Oxford University Press, p.270. Shaw, *op.cit*. p. 28 and p. 1284

[665] Nussbaum, A. (1947), *A Concise History of the Law of Nations*, New York: MacMilllan, pp. 251–90.Shaw, *Ibid*., p.30. Neff, *op.cit.,* p.50

[666] Shaw, *op.cit*., p. 31. Neff, *op.cit*., p. 51

[667] "The Statute of the International Court of Justice", Available at: http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0#CHAPTER_II (Accessed at: 22/08/2012)

The International Court of Justice (ICJ) description of sources of international law was widely recognised by the international community.[668] The establishment of the Nuremberg and Tokyo Tribunals by the Allies was:

> *"Recognition of individual responsibility under international law without the usual interposition of the state and has been reinforced with the establishment of the Yugoslav and Rwanda War Crimes Tribunals in the mid-1990s and the International Criminal Court in 1998."*[669]

With the founding of the UN, new threat perceptions and problems began to be identified by the Security Council and the General Assembly, and since 1963, there have been 14 international agreements and four amendments to combat terrorism and terrorist attacks.[670]

With the adoption of the Universal Declaration of Human Rights[671] by the UN, universal human rights were accepted as important, and some interventions were made by countries to protect people and human rights, such as those in Kosovo in 1999, and Libya in 2011. Furthermore, the International Covenant on Economic and Social and Cultural Rights[672] and the International Covenant on Civil and Political Rights[673] were signed in 1966, and came into force in 1976.

Humanitarian interventions [674] by the UN and NATO, have prompting some scholars to argue about the legality of the intervention in terms of evaluating the situation from their own theoretical viewpoints.[675] For instance, the positivist supporter might accept a case as legal,

[668] Shaw, *op.cit.*, p.70

[669] Shaw, *op.cit.*, p. 46

[670] "International Legal Instruments to Counter Terrorism", Available at: http://www.un.org/terrorism/instruments.shtml (Accessed at 23/08/2012)

[671] "The Universal Declaration of Human Rights", Available at: http://www.un.org/en/documents/udhr/ (Accessed at: 23/08/2012)

[672] "International Covenant on Economic, Social and Cultural Rights", Available at: http://www2.ohchr.org/english/law/cescr.htm (Accessed at:23/08/2012)

[673] "International Covenant on Civil and Political Rights", Available at: http://www2.ohchr.org/english/law/ccpr.htm (Accessed at: 23/08/2012)

[674] NATO's definition, adopted in Scheveningen in November 1999, stated that: "*A humanitarian intervention is an armed intervention in another state, without the agreement of that state, to address (the threat of) a humanitarian disaster, in particular caused by grave and large-scale violations of fundamental human rights".* Roberts, G. W. (2000), "Humanitarian Intervention: Definitions and Criteria", *Centre for Strategic Studies,* Vol. 3, Part 1, Available at: http://www.victoria.ac.nz/css/docs/strategic_briefing_papers/vol.3%20jun%202000/hi.pdf (Accessed at: 27/08/2012). Humanitarian intervention is also defined as: "*The threat or use of force by a state, group of states, or international organisation primarily for the purpose of protecting the nationals of the target state from widespread deprivations of internationally recognized human rights".* Murphy, S. D. (1996), *Humanitarian Intervention: The United Nations in an Evolving World Order,* Philadelphia: University of Pennsylvania Press, p.12

[675] I used scholars because all theorists evaluate international law differently and therefore I used general mean of scholars.

but realists or others might view it as illegal, so it is essential to evaluate cases in the light of theories.

According to Onuf, *"as doctrine, legal positivism rests on three pillars: 1) international law has fixed sources (rules for making rules), 2) subjects (rightful participants in the system of rules) and 3) sanctions (rules for securing compliance with rules).*[676] According to Gontarek, "*various legal scholars have propounded arguments supporting positivism or naturalism as the basis for all law and these arguments are often plausible, until they are applied to international law…thus, both positivist and naturalist theories are wanting as means of explaining the origins and force of international law. Positivism does not address the intangible sources that are inevitable in a system of law that aspires to govern equal sovereigns; naturalism lacks the visibility and uniformity necessary to define what the law really is, especially across highly diverse cultures and national legal systems… a move away from a simple choice of positivist or naturalist views of international law derives from the inability of either to accommodate the diversity within this body of law. Intuitively, a hybrid positivist/naturalist perspective that captures the advantages of both has attractive qualities*"[677]. Gontarek continues, "*The difficulty inherent in achieving a balance of objective and subjective features within a single legal theory is obvious. A contractarian perspective offers insight into some forms of international law arise and are respected or violated but this view has weaknesses, specifically for vague forms such as writings, equity, and natural law. An economic conceptual framework may prove to be the most practical analytic tool for international law. Its usefulness is independent of the form of law and it can inform estimates of future behaviour with considerable force. It goes beyond obligation and engages behaviour at the very fundamental level of reward and punishment. An economic perspective can gauge intensity or the absence of motivation and allows nations to predict the effect of changes in the environment on compliance.*"[678] Also, Bettenhausen states that "*one useful application of economic analysis to international positivism might be a contractarian analysis of informal constraints on contracting parties. The concepts - expectation of repeat dealings, reputation within the community, and the availability of accurate information about the other party and the subject of the contract - provide an economic explanation of why*

[676] Tascan, J., Onuf, N., and Parisi, F. (1995), "International Legal Theory", *Publication of the American Society of International Law Interest Group on the Theory of International Law,* Volume 1(1), Available at: https://law.ubalt.edu/centers/cicl/publications/docs/ILT_01_1_1995.pdf (Accessed at: 03/12/2015)

[677] *Ibid.*

[678] *Ibid.*

states may feel obligated to follow customary international law even with the absence of express consent or formal enforcement mechanisms."[679]

In this thesis I will introduce Game Theory as a hybrid of these theories. Both positivism and natural law accept self-defence as the exception of the prohibition of the use of force[680]. This understanding is also supported by the Game Theory under the Nash Equilibrium. According to Ohlin, "*the Nash Equilibrium here is clear. The norm in question is the legal prohibition on the use of force, by both the UN Charter and customary law, unless such use of force is taken in self-defence or authorized by the Security Council - the central clearing house for decisions regarding international peace and security…In the current scheme, the prohibition against the use of force is now coupled with the Security Council's authority to authorize use of force to restore international peace and security*."[681]

4.2. The Prohibition of the Use of Force

The UN Charter governs the basic rules of using force in international law. It does not allow member states to use force whenever they want.[682] Article 2(4) of the Charter explains this as follows: "*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*"[683] According to Gray, the International Court of Justice (ICJ) accepts Article 2(4) as a cornerstone of the UN Charter in

[679] *Ibid*.

[680] For more information; Tams, C. J. and Tzanakopoulos, A. (2014), "Use of Force", in Kammerhofer, J. and D'Aspremont, J. (eds.) (2014), *International Legal Positivism in a Post-Modern World*, Cambridge: Cambridge University Press. Kleimann, D. (2006), "Positivism, the New Haven School, and the Use of Force in International Law", *Brussels Journal of International Studies*, Vol. 3, Available at: https://www.kent.ac.uk/brussels/documents/journal/2006/David%20Kleimann%20-%20Positivism%20the%20New%20Haven%20School%20and%20the (Accessed at: 03/12/2015). Merriam, M. J. J. (2010), "Natural Law and Self-Defense", *Military Law Review*, Vol. 206, Available at: http://poseidon01.ssrn.com/delivery.php?ID=253020073123121008114081107025012028059064002079017045002024010027112068127012004078097103011016022127108107074127089123116127117039004050076082105100096078106084090068005079103118082085112004002094070080107123098109109007019101091095027113118083081003&EXT=pdf (Accessed at: 03/12/2015). Bowett, D. W. (1958), *Self-Defence in International Law*, Manchester: Manchester University Press

[681] Ohlin, J. D. (2015), *The Assault on International Law*, Oxford: Oxford University Press, p. 99

[682] Başeren, S. H. (2003), *Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmasının Sırları*, Ankara: Ankara Üniversitesi Basımevi, p. 46

[683] "The United Nations Charter", *op.cit*. Also see, Simma, B. (1999), "NATO and the UN and the Use of Force: Legal Aspects", *European Journal of International Law*, Available at: http://ejil.oxfordjournals.org/content/10/1/1.full.pdf+html (Accessed at: 10/06/2014), pp. 2-3

not permitting the use of force in any territory.[684] Additionally, he states that, since it is not a treaty obligation, it is a customary law, or *jus cogens* for the international community.[685]

In 1970 the General Assembly adopted, "The Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations," which interprets Article 2(4) of the Charter as follows:

- *A war of aggression constitutes a crime against the peace, for which there is responsibility under international law.*
- *In accordance with the purposes and principles of the United Nations, States have the duty to refrain from propaganda for wars of aggression.*
- *Every State has the duty to refrain from the threat or use of force to violate the existing international boundaries of another State or as a means of solving international disputes, including territorial disputes and problems concerning frontiers of States.*
- *Every State likewise has the duty to refrain from the threat or use of force to violate international lines of demarcation, such as armistice lines, established by or pursuant to an international agreement to which it is a party or which it is otherwise bound to respect. Nothing in the foregoing shall be construed as prejudicing the positions of the parties concerned with regard to the status and effects of such lines under their special regimes or as affecting their temporary character.*
- *States have a duty to refrain from acts of reprisal involving the use of force.*
- *Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of their right to self-determination and freedom and independence.*
- *Every State has the duty to refrain from organizing or encouraging the organisation of irregular forces or armed bands including mercenaries, for incursion into the territory of another State.*

[684] Gray, C. D. (2008), *International Law and The Use of Force,* Oxford: Oxford University Press, p. 30

[685] *Ibid.* ; See also; Arend, A. C. and Beck, R. J. (2013), *International Law and The Use of Force,* New York: Routledge, p. 1. Bothe, M. (1967), "Consequences of the Prohibition of the Use of Force: Comments on Arts 49 and 70 of the ILC's 1966 Draft Articles on the Law of Treaties", *Heidelberg Journal of International Law,* Available at: http://www.zaoerv.de/27_1967/27_1967_3_c_507_519.pdf (Accessed at: 10/06/2014), p. 508. Shaw, *op.cit.*, p. 1123

- *Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.*
- *The territory of a State shall not be the object of military occupation resulting from the use of force in contravention of the provisions of the Charter. The territory of a State shall not be the object of acquisition by another State resulting from the threat or use of force. No territorial acquisition resulting from the threat or use of force shall be recognized as legal. Nothing in the foregoing shall be construed as affecting:*

a) Provisions of the Charter or any international agreement prior to the Charter regime and valid under international law; or

b) The powers of the Security Council under the Charter.

- *All States shall pursue in good faith negotiations for the early conclusion of a universal treaty on general and complete disarmament under effective international control and strive to adopt appropriate measures to reduce international tensions and strengthen confidence among States.*
- *All States shall comply in good faith with their obligations under the generally recognized principles and rules of international law with respect to the maintenance of international peace and security, and shall endeavour to make the United Nations security system based on the Charter more effective.*[686]

Article 10 of the Charter provides: "*The General Assembly may discuss any questions or any matters within the scope of the present Charter or relating to the powers and functions of any organs provided for in the present Charter, and, except as provided in Article 12, may make recommendations to the Members of the United Nations or to the Security Council or to both on any such questions or matters*."[687] Therefore the General Assembly can only make recommendations; the Security Council's duty, on the other hand, is distinct in terms of taking decisions and applying them. According to Article 25 of the Charter, "*The Members of*

[686] The United Nations General Assembly (1970), *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, Available at: http://www.un-documents.net/a25r2625.htm (Accessed at: 10/06/2014)

[687] "The UN Charter", *op.cit.*

the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter."[688] Therefore, the Declaration can only be accepted as an interpretation of Article 2(4) without any binding rules.[689]

Finally, the use of force in terms of aggression and land reclamation is prohibited by the UN under Article 2(4) of the Charter.[690] Shaw states that Article 2(4) not only covers armed force, but also economic forces as well.[691] Because there is no clear description of the type of threat or uses of force in Article 2(4) of the Charter, it could support a view that it includes economic and political sanctions as threats or uses of force against states.[692] This suggests a fairly broad interpretation of the Article; however the introduction of the Charter states that the, "use of force" means armed force. It reads as follows: "*to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest...*"[693] This points to a strict interpretation limiting the use of force to armed force. It is this narrow interpretation that may limit any response to situations that may amount to cyber terrorism suggesting that a broader interpretive approach may now be necessary.

4.3. Exceptions to the Prohibition of the Use of Force

There are only two exceptions to the prohibition of the use of force: viz., self-defence and the UN Security Council's passing a resolution.[694]

4.3.1. The Right of Self-Defence

The main exception to the prohibition of the use of force in Article 2(4) of the UN Charter is self-defence. Furthermore, Article 51 of the UN Charter stipulates the right to self-defence. According to that Article:

> *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken*

[688] *Ibid.*

[689] Shaw, *op.cit.*

[690] Yayla, M. (2013), "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", *TBB Dergisi*, Vol. 107, Available at: http://tbbdergisi.barobirlik.org.tr/m2013-107-1293 (Accessed at: 12/06/2014), p. 204

[691] Shaw, *op.cit.*, p. 1124

[692] Yayla, *op.cit.*, p. 205

[693] "The United Nations Charter", *op.cit.*

[694] Evans, G. (2004), *International Law and the United Nations: The Use of Military Force*, Available at: http://www.gevans.org/speeches/speech106.html (Accessed at: 15/01/2015). Stürchler, N. (2007), *The Threat of Force in International Law*, Cambridge: Cambridge University Press, p. 85

> *measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such actions as it deems necessary in order to maintain or restore international peace and security."*[695]

States can only apply to Article 51 when they are the victims of armed attacks.[696] For example following the use of military force against Nicaragua and intervening in Nicaragua's internal affairs by the USA,[697] the ICJ stated:

> *"...an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description, contained in Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law."*[698]

The ICJ's decision regarding the Nicaraguan case suggests that where a state's relies on its right to self-defence states must, "*distinguish the gravest forms of the use of force (those constituting an armed attack) from other less grave forms.*"[699] Green interprets the ICJ's decision as signifying that "*the responding state must face an attack of a 'grave' level, beyond that of a use of force simpliciter.*"[700] This means that the states cannot use their right

[695] "The UN Charter", *op.cit.*

[696] O'Connell, M. E. and Molla, R. E. (2013), "The Prohibition on the Use of Force for Arms Control: The Case of Iran's Nuclear Program", *Penn State Journal of Law&International Affairs*, Vol. 2(2), Available at: http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1056&context=jlia (Accessed at: 15/01/2015), p. 316. International Court of Justice (1986), *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Available at: http://www.icj-cij.org/docket/files/70/6503.pdf (Accessed at: 15/01/2015), p. 93

[697] After the judgment, the ICJ held that the USA had violated international law. For more details, see: International Court of Justice (1984), *Application Instituting Proceedings filed the Registry of the Court on 9 April 1984: Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, Available at: http://www.icj-cij.org/docket/files/70/9615.pdf (Accessed at: 30/08/2015)

[698] *Ibid*., paragraph 195; See also; Public International Law, *Lesson 5.4. Second Exception to the Prohibition on the Use of Force: Right of Self-Defence*, Available at: https://ruwanthikagunaratne.wordpress.com/2011/04/12/article-51-un-charter/ (Accessed at: 15/01/2015)

[699] *Ibid*. Prg. 191

[700] Green, J. A. and Grimal, F. (2012), "The Threat of Force as an Action in Self-Defense Under International Law", *Vanderbilt Journal of Transnational Law*, Vol. 44, Available at: http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/green-cr.pdf (Accessed at:06/01/2015), p. 300

of self-defence against any force if it is not an “an armed force.” Kassimeris and Buckley suggest that, “*only the gravest uses of force (‘armed attacks’) allow the victim State to use military force in response….in general, though, this simply means that comparatively minor instances of force (such as an isolated border skirmish, for example), will not trigger the right of self-defence in and of themselves*.”[701] There are, therefore, strict limitations on how a state may use force in any case.

Article 5 of the North Atlantic Treaty provides that NATO can protect its members from any threat or use of force aimed against them:

> *“The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.*
>
> *Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.”*[702]

Clearly, one of the main aims of both NATO and the UN is to protect its members from any threat or use of force. Additionally, NATO can also invoke the UN Charter as a justification for using self-defence against attacking states.

To sum up, even though states have the right to self-defence whenever an armed attack is made against their territory, they must report the situation to the UN Security Council in order to take any measures against the attacking states. It can be accepted that international law protects states against any acts of aggression made against them, and gives them the right to protect themselves against any armed forces.

[701] Kassimeris, G. & Buckley, J. (2010), *The Ashgate Research Companion to Modern Warfare*, Farnham: Ashgate Publishing Limited, p. 296

[702] “The North Atlantic Treaty”, *op.cit.*

4.3.2. Under the Resolutions of the UN Security Council

The other exception to the prohibition of the use of force is that of resolutions passed by the UN Security Council. The UN Charter meted out the responsibility of protecting the peace and security of the world to the UN Security Council in Article 24 which provides that[703]:

> "*[i]n order to ensure prompt and effective action by the United Nations, its Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf.*"[704]

As signatories to the Article, the member states of the UN accepted the role and power of the Security Council. Article 24(2) of the Charter states how the Security Council conducts its duties, "*in discharging these duties the Security Council shall act in accordance with the Purposes and Principles of the United Nations. The specific powers granted to the Security Council for the discharge of these duties are laid down in Chapters VI, VII, VIII, and XII.*"[705] Chapter VII of the Charter, entitled "Action with Respects to Threats to the Peace, Breaches of the Peace, and Acts of Aggression", lays out the duties of the Security Council in maintaining peace and security in the international arena.

According to Article 39 of the Charter, "*[t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security*."[706] Although the Article describes the duties of the Security Council, the Charter does not state which cases or situations are to be regarded as a threat to, or breach of, the peace. According to Schmidt, "*the lack of definitions is not accidental. The struggle for the definition of 'aggression' has been a long and continuous one..... The question as to what acts are included in the term 'breach of the peace' in Article 39 is even more difficult. It is, however, clear that this term is broader than the term 'act of aggression', since the latter is covered by the former.*"[707] Since

[703] Gray, C. (2003), "The Use of Force and The International Legal Order", in Evans, M. (2003), *International Law*, Oxford: Oxford University Press, p. 607

[704] "The United Nations Charter", *op.cit.*

[705] *Ibid.*

[706] *Ibid.*

[707] Schmidt, H. K. (1958), "The Charter of the United Nations: An Instrument to Re-Establish International Peace and Security?", *Indiana Law Journal*, Vol. 33(3), Available at: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2885&context=ilj (Accessed at: 18/02/2015), p. 323

the members accept the decisions made by the Security Council, individual states may have no right to speak about the decisions passed by the Security Council. Article 25 of the Charter provides that, "*The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter"*[708] According to Calvan, "*the decisions taken by the Security Council have a binding character, so they must be carried out by all Member States in accordance with Article 25 of the UN Charter."*[709] Additionally, Schmidt states that "*[t]his provision is further strengthened by Article 25 by which members of the organisation are bound to accept the decisions of the Security Council."*[710] Accordingly the Security Council has overall responsibility to take a decision about the threats, and states cannot argue against these decisions.

The Security Council always calls on both sides of any given conflict to take provisional measures before making any decisions or recommendations. Article 40 of the Charter stipulates that, "*[i]n order to prevent an aggravation of the situation, the Security Council may, before making the recommendations or deciding upon the measures provided for in Article 39, call upon the parties concerned to comply with such provisional measures as it deems necessary or desirable. Such provisional measures shall be without prejudice to the rights, claims, or position of the parties concerned. The Security Council shall duly take account of failure to comply with such provisional measures."*[711] Even though the Charter does not lay out any of the provisional measures it refers to here, Yayla lists the various provisional measures that they can take as calling for an end to the conflict, calling for a ceasefire, or ordering the withdrawal of armed force.[712]

Article 41 of the Charter regulates the measures which do not include the use of armed force, it provides that:

> "*The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."*[713]

[708] "The United Nations Charter", *op.cit.*

[709] Galvan, *op.cit.*, p. 151

[710] Schmidt, *op.cit.*, p. 322

[711] "The United Nations Charter", *op.cit.*

[712] Yayla, *op.cit.*

[713] "The United Nations Charter", *op.cit.*

The main aim of Article 41 is to end conflicts without the use of armed force. According to Gray, "*[t]he official position is that Article 41 measures are not punishment but should be designed to secure compliance with decisions of the Security Council.*"[714]

If the measures taken by Article 41 are insufficient, the Security Council can apply Article 42 for the purpose of maintaining international peace and security:

> *"Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations*."[715]

There are, therefore, many steps that the Security Council may use in order to maintain peace and security, including armed force. The UN Charter does not give direct permission to individual states to use force against attackers for the purpose of maintaining peace and security.

In sum, the Security Council has the primary role of protecting international peace and security. If it determines that a threat to peace, a breach of the peace, or an act of aggression has been carried out, the Security Council may apply the rules of Chapter VII to maintain international peace and security. Until the decision and recommendations of the Security Council are passed, states cannot utilise their armed forces, or call for the right to self-defence. The use of armed force is the last step which can possibly be made in order to maintain international peace and security under the UN Charter. Galvan states that, "[t]*he Security Council is the only organ with the power to take enforcement action that can involve military force, [and] notwithstanding this power, a determination of Article 39 has to be done before the Security Council determines to apply it.*"[716] If Article 39 does not solve the problem, then Articles 40, 41, and, lastly, 42 should be implemented before finally resorting to the use of armed force.

[714] Gray (2003), *op.cit.*, p. 608

[715] "The United Nations Charter", *op.cit.*

[716] Galvan, *op.cit.*, p. 153

4.4. International Law Relating to Cyber Attacks

The United Nations General Assembly explained what cyberspace freedom for all states meant in 1981.[717] The "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States" affirms that:

> *"the right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, inter alia, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order."*[718]

This suggests that the UN General Assembly has established a non-intervention area for all states, according to Roscini, the Declaration not only covers cyber-attacks, but, also computer network operations (CNE) which could also, depending on circumstances, be regarded as unlawful intervention, which includes cyber propaganda and the defacement of websites.[719] In addition, the United Nations General Assembly issued "Guidelines for the Regulation of Computerized Personal Data Files" in 1990.[720] According to these guidelines, necessary measures should be taken in order to protect personal data files against any threats, including natural and human dangers.[721]

The only multilateral convention against cybercrime is the "2001 Council of Europe Convention on Cybercrime."[722] Since coming into force on 1 July, 2004,[723] it has been seen as a cornerstone for member states in the European Union. Several non-member States in the Council of Europe, such as Canada, Japan and South Africa also signed the convention. Moreover, it was also ratified by the United States, where it came into force on 1 January, 2007.[724] This convention invites member states to align their national laws and adopt legal tools for certain procedural matters for the purpose of strengthening the capacities of public

[717] Roscini, M. (2010), "World Wide Warfare-Jus ad bellum and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law,* Vol. 14, Available at: http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf (Accessed at: 10/05/2015), p. 103

[718] The United Nations General Assembly, (1981), *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, A/RES/36/103,* Available at: http://www.un.org/documents/ga/res/36/a36r103.htm (Accessed at: 15/05/2015)

[719] Roscini, *op.cit*., p. 103

[720] The United Nations General Assembly (1990), *Guidelines for the Regulation of Computerized Personal Data Files, A*vailable at: http://www.un.org/documents/ga/res/45/a45r095.htm (Accessed at: 20/05/2015)

[721] *Ibid*.

[722] Council of Europe (2001), *Convention on Cybercrime,* Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (Accessed at: 15/05/2015)

[723] Vatis, M. A. (2010), *The Council of Europe Convention on Cybercrime,* Available at: http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf (Accessed at: 20/05/2015), p. 209

[724] *Ibid*.

prosecution offices, in order to better conduct inquiries and collect evidence with regards to cybercrime. The "Additional Protocol to the Convention on Cybercrime" was also adopted in 2006,[725] by which signatory states are bound to criminalise racist or xenophobic material published online.

Article 2 of the UN Charter specifically stipulates that *"all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*."[726] This means that all states should be free to choose their own political, social and cultural systems, and that others cannot interfere with those choices.

It is not easy to explain and evaluate all cyber-attacks as threats or as uses of force against territorial integrity. According to Roscini,*"…the threat of a use of force with traditional weapons communicated through cyber means. Article 2/4 does not specify the methods through which a threat should be carried out and thus communicating a threat via the Internet would be on the same theoretical footing as communicating a threat by traditional methods. The cyber threat could also warn of a possible cyber-attack by the threatening state. Whether this is a threat under Article 2/4 depends on whether the use of (cyber) force envisaged in the threat is unlawful. Indeed in its 1996 Advisory Opinion on the Legality of the Use of Nuclear Weapons, the ICJ linked the legality of threats to the legality of the use of force in the same circumstances."*[727]

Therefore cyber force can be regarded as force that can be evaluated under Article 2/4 of the UN Charter. The Tallinn Manual on the International Law Applicable to Cyber Warfare[728] mentions that *"a state may exercise control over cyber infrastructure and activities within its sovereign territory,"*[729] emphasising state sovereignty over their own cyber infrastructures, making any attack on these infrastructures unlawful.

Although states and international organisations have faced several cyber-attacks, the international community has not still had a consensus to address the attacks through the use of international law (e.g. *What circumstances can be accepted as an act of war by the*

[725] Council of Europe (2001), *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, Available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=189 (Accessed at: 15/05/2015)

[726] "The United Nations Charter", *op.cit.*

[727] Roscini, *op.cit*., p. 104

[728] These documents were prepared by the CCDCOE. They do not have any binding rules on the states.

[729] Schmitt, M. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press, Rule 1, p. 15

international community?[730] and *When would a cyber-attack rise to the level of an armed attack justifying self-defence under Article 51 of the U.N. Charter?)*[731] There are differences of opinion for example, Howard Schmidt,[732] believes that cyber-attacks cannot be accepted as acts of war, in contrast Ronald Deibert[733] suggests that they could be classed as acts of war, providing the cases of Estonia, Georgia and Iran as examples. Despite their disagreement both address these attacks through international law and the law of conflict; for both, a State which is attacked on its own territory can invoke Article 51 of the United Nations Charter,[734] citing self-defence as a justifiable reason for going to war. These arguments continue amongst the members of the international community, as do arguments over the definition of cyber terrorism itself.[735]

Article 31/1 of the 1969 Vienna Convention on the Law of Treaties stresses the importance of interpreting and evaluating bilateral, multilateral or international agreements and treaties in good faith, it states: "*[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.*"[736] Moreover, according to Silver, "*The historical background of Article 2(4) shows that it was conceived against a background of international efforts to eliminate unilateral recourse to armed force. Measures of economic and political coercion were not the issue*."[737] Schmitt explains and interprets Article 2/4 as follows:

[730] Shackelford (2009), *op.cit.*, p. 38

[731] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlani A., Perdue, W., Spiegel, J. (2012), "The Law of Cyber-Attack," *California Law Review*, Available at: http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf (Accessed at: 05/05/2015), p. 26; See also; Roscini, *op.cit.*, p. 114

[732] Yayla, *op.cit.*, p. 188.

[733] *Ibid*.

[734] Article 51 of the United Nations Charter reads as follows: 'Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.' Available at: http://www.un.org/en/documents/charter/chapter7.shtml (Accessed at: 05/04/2013)

[735] Yayla, *op.cit*.

[736] "1969 Vienna Convention on the Law of Treaties", Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf (Accessed at: 16/05/2015); See also; Cohen, A. (2010), "Cyberterrorism: Are We Legally Ready," *The Journal of International Business and Law*, Available at: https://law.hofstra.edu/pdf/Academics/Journals/JIBL/JIBL_vol9no1_Cohen_Cyberterrorism.pdf (Accessed at: 16/05/2015), pp. 12-13

[737] Silver, D. B. (2002), "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," *International Law Studies*, Vol. 76, Available at: https://www.usnwc.edu/Research---Gaming/International-Law/New-International-Law-Studies-(Blue-Book)-Series/International-Law-Blue-Book-Articles.aspx?Volume=76, (Accessed at: 16/05/2015), p. 81

> "'*Force' appears, as in Article 2/4, without the qualifier 'armed' but, as demonstrated by the reference to 'armed forces,' clearly contemplates that the force used be armed. The Charter uses the term 'armed force' twice [—] a fact which might seem to suggest the drafters intended to distinguish it from unqualified force after all. However both cases involve Chapter VII enforcement, in which armed force is but one of multiple options available to the Security Council in responding to threats to the peace, breach of the peace, or acts of aggression. Read in context, they clearly refer to a particular point along the continuum of coercion. By contrast, because Article 2(4) precludes nothing but 'force' there was no need to distinguish it through qualification."*[738]

Silver points out that there is no resolution of the International Court of Justice concerning the acceptance of political and economic coercions under Article 2/4.[739] Since Article 2/4 of the UN Charter only refers to armed force, it is difficult, if not impossible, to interpret this article to include political and economic coercion as armed force. But there is no common agreement on the application of Article 2/4. Roscini states that one interpretation capable of covering cyber force (attacks) would be that, if an unauthorised military (or cyber force) of one state attacks another state for the purpose of causing the destabilisation of the country, this would be a violation of that article.[740] Roscini points to the Vienna Convention as evidence. Article 31/3/b speaks of, "*any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation*."[741] Roscini interpretation is correct insofar as, nowadays, many states have established their own cyber forces. Furthermore, these states have attempted to create new laws regarding cybercrime and cyber-attacks. Some of them, such as the USA and the UK, regard cyber-attacks as a form of armed force and I suggest that international law must be interpreted broadly in order to cover the new cyber threats facing the international community.

Hathaway *et al.* accept that not all cyber-attacks should be considered as armed attacks but they identify three types of cyber-attack can be accepted as an armed attack, allowing for

[738] Schmitt, M. (1999), "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, pp. 904-905

[739] Silver, *op.cit;* See also; Schmitt (1999), *Ibid*., pp. 905-908, and Roscini, *op.cit*., p. 105

[740] Roscini, *op.cit*., pp. 107-108

[741] "1969 Vienna Convention on the Law of Treaties," *op.cit*., and *Ibid*, p. 108

self-defence: 1) the instrument-based approach; 2) the target-based approach; and 3) the effects-based approach.[742]

Schmitt suggests that:

> "[The] u*se of force paradigm has been instrument-based; determination of whether or not the standard has been breached depends on the type of the coercive instrument-diplomatic, economic, and military-selected to attain the national objective in question. The first type of instruments might arise to the level of intervention, but they do not engage the normatively more flagrant act of using force. However, despite instrument classing, in actual practice it does not follow that coercive acts involving armed force necessarily operate at counter-purposes with community values."*[743]

It is difficult to see cyber-attacks being classified as belonging to this type of approach, instrument-based, suggesting that it cannot be addressed by the application of Article 51 of the UN Charter because, it does not use traditional military weapons.[744] This approach is best used when an armed attack is conducted or armed force is used only if the military weapons used. Hathaway and *et. al.* give an example of this type of approach as: "*bombing computer servers or Internet cables could meet the requirements of an armed attack, for example, if the strike was of sufficient gravity*".[745]

The target-based approach is a cyber-attack whose main aim is to harm critical computer systems. According to Hathaway *et al.*, "*the primary aim of this approach is to determine when a cyber-attack portends imminent and sufficient harm to justify the use of anticipatory self-defence in response."*[746] This approach identifies national and international critical infrastructures as being important. Thus, if any attack targets these systems, self-defence can be used in order to justify a state's fighting back against such an attack.

The effects-based approach categorises cyber-attacks in terms of the severity. If the cyber-attacks causes severe harm, this can be regarded as an armed attack. Thus cyber-attacks

[742] Hathaway *et.al., op.cit.*, pp. 31-32; See also; Graham, D. E. (2010), "Cyber Threats and the Law of War," *Journal of National Security Law and Policy*, Vol. 4 (87), Available at: http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf (Accessed at: 13/05/2015), pp. 91-92

[743] Schmitt (1999), *op.cit.,* p. 909

[744] *Hathaway et.al., op.cit..*, p. 32. Also, Hollis explains this situation in his work as: "the classic "instrumentality" approach argues Information Operations does not qualify as armed force because it lacks the physical characteristics traditionally associated with military coercion.71 The text of the U.N. Charter offers some support for this view; Article 41 lists "measures not involving the use of armed force" to include "complete or partial interruption of . . . telegraphic, radio, and other means of communication." Hollis, D. B. (2007), "Why States Need an International Law for Information Operations", *Lewis &Clark Law Review*, Vol. 11(4), Available at: http://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf (Accessed at: 20/05/2016), p. 1041

[745] *Ibid*., p. 33.

[746] *Ibid*.

would be classified in terms of the harm created and their length, but it may be problematic to identifying which cyber-attacks should be regarded as armed attacks. Hathaway *et al*. provide the following useful examples: "*an attack on an air traffic control system, an attack that disables a regional electrical power grid, an attack on the New York Stock Exchange or national financial networks, or the 2007 cyber-attack on prominent Estonian websites.*"[747] These types of cyber-attack are obviously at the serious end of the spectrum with the possibility of causing severe harm to infrastructure and potentially leading to civilian deaths. It is for this reason that they must be accepted as armed attacks.

Schmitt explains six ways in which cyber-attacks can be considered armed attacks:[748]

> *1) severity, the type and scale of the harm; 2) immediacy, how quickly the harm materializes after the attack; 3)directness, the length of the causal chain between the attack and the harm; 4)invasiveness, the degree to which the attack penetrates the victim state's territory; 5) measurability, the degree to which the harm can be quantified; and 6) presumptive legitimacy, the weight given to the fact that, in the field of cyber-activities as a whole, cyber-attacks constituting an armed attack are the exception rather than the rule.*[749]

Schmitt's explanation and application of the six rules attempts to explain which cyber-attacks should be accepted as an armed force or attack. By contrast, Silver invokes the rule of severity, reasoning that only severity can explain when a cyber-attack can be accepted as being an armed attack:

> *"severity, as defined for this purpose, seems applicable only to physical injury and property damage, compelling the conclusion that CNA will be considered within the force category only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion. In short, what seems at first blush to be a nuanced way of analysing incidents of CNA in practice may in fact tum out to do no more than identify the cases that would be clear without applying a criterion any more formal than was suggested in the preliminary conclusions above: CNA will be considered as force when it*

[747] *Ibid*, p. 34.
[748] Quoted in Hathaway *et.al., op.cit.*, p. 34
[749] Hathaway *et.al., op.cit.*, p. 34

> *causes physical injury or property damage that is recognizably similar to that produced by instruments generally identified as weapons*."[750]

It is crucial to clarify when states should apply Article 51 of the UN Charter when faced with a cyber-attack. As previously discussed, states can use the right of self-defence only when they are facing an armed attack, or when the Security Council passes a resolution stating that a particular attack was an armed one. In this context Article 51 is clearer than Article 2/4,[751] since it provides that, if the states do not encounter any armed force, they are not able to claim the right of self-defence.

In summary, cyber-attacks can be considered under the purview of Article 2/4 of the UN Charter because, cyber threats have a potential to create big problems for the international community and if cyber-attacks can be considered under Article 2/4 of the UN Charter, the UN role may have a deterrent effect against the attackers. Some states did not choose to use traditional military weapons when attacking another state, as was the case of Estonia. Yet if a state is attacked in such a way, this does not mean that it can apply directly to the right of self-defence. Both Schmitt and Silver are clear, if an attack causes death or damage to property, that attack should be considered under Article 51 of the UN Charter; but that other attacks, such as defacement of websites or hacking, cannot be classified as being of an armed character, so as to protect the peace and security of the world.

4.5. Conclusion

The use of force is prohibited under the UN Charter, with only two exceptions: self-defence and the use of force under a resolution of the Security Council. Today the main problem regarding the use of force is how it can be applied to new and emerging threat perceptions. The lack of a common definition of cyber terrorism has the potential to cause interpretive and application problems for international law. There are many opinions about the application of Articles 2/4 and 51 of the UN Charter. Some accept cyber-attacks as being a type of armed force, but others do not.[752] This creates a problem of definition. If the international community is not successful in finding a solution (i.e. identifying and describing the problem and applying definitions to international law), the international community and organisations will not be able to resolve their other problems (e.g. terrorism and humanitarian problems).

[750] Silver, *op.cit*., pp. 90-91

[751] Schmitt, (1999), *op.cit*, p. 928

[752] See Footnote 4

It is imperative that a common definition is agreed. If the international community is able to solve this first problem, the other problems could also, in turn, be solved. But more important than definitions, is to application of the international law. The suggestion is that, in terms of applying laws to cyber-attacks, the international community should adopt Schmitt’s and Silver’s approach that argues that cyber-attacks should be considered as armed force only when the cyber-attacks cause severe harm to infrastructure and potentially leading to civilian deaths. It may also assist in addressing legal questions about the nature of attack and the method or criteria for determining if it is credible enough to base a reasonable decision to act or not to act on. This, in turn, will direct, and provide a degree of consistency in how the international community applies international law to cyber-attacks.

CHAPTER 5: THE CYBER SECURITY POLICY OF NATO

5.1. Introduction

NATO's policy will be critically analysed and evaluated since the acceptation of the first cyber security policy in this chapter. In addition, the policy will be evaluated using Game Theory in an attempt to understand and evaluate NATO's policy.

During the second chapter, the concept of threat was detailed and analysed, and an important shift in the changing nature from threat to risk was also stated. NATO has adopted new Strategic concepts to determine new threats, risks and uncertainties in the international arena, in order to survive. NATO has also extended its operational capability to non-member countries to protect both its members and other countries from any kind of threat or risk.

With the improvement of technology, new risks and threats have emerged. In accordance with the technological improvement, human existence has become indexed to technology. More than two billion people now use the Internet[753] and many states have Supervisory Control and Data Acquisition (SCADA) systems in their territories.[754] These developments illustrate the importance of cyber security policies for states, and regional and international organisations. In the context of cyber terrorism, these information and communication technologies have created new challenges for NATO, because the increasing reliance by its member states on technology has had a fundamental and pervasive influence on various aspects of cyber terrorism and the ability of the international community to address it, changing the way in which NATO should identify mainstream security concerns.

Whilst NATO faced its first cyber-attack in 1999 it was the attack on Estonia that showed NATO the reality of cyber threats, and the necessity to provide protection from these types of

[753] "Internet Usage Statistics", Available at: http://www.internetworldstats.com/stats.htm (Accessed at: 01/06/2014)

[754] SCADA systems are described as: "an industrial control system at the core of many modern industries such as manufacturing, energy, water, power, transportation and many more. SCADA systems deploy multiple technologies that allow organisations to monitor, gather, and process data as well as send commands to those points that are transmitting data. Virtually anywhere you look in today's world, you will find some version of a SCADA system running, whether it's at your local supermarket, refinery, waste water treatment plant, or even your own home. SCADA systems range from simple configurations to large, complex projects. Most SCADA systems utilize HMI (human-machine interface) software that allows users to interact with and control the machines and devices that the HMI is connected to such as valves, pumps, motors, and much more. SCADA software receives its information from RTUs (remote terminal units) or PLCs (programmable logic controllers) which can receive their information from sensors or manually inputted values. From here, the data can be used to effectively monitor, collect and analyze data, which can potentially reduce waste and improve efficiency resulting in savings of both time and money. Numerous case studies have been published highlighting the benefits and savings of using a modern SCADA software solution such as Ignition." Inductive Automation defines SCADA systems as, "*SCADA (supervisory control and data acquisition)* "What is SCADA", Available at: https://www.inductiveautomation.com/what-is-scada (Accessed at: 16/09/2014)

attacks and to obstruct such threats whenever possible. In response NATO has developed plans and policies to improve its own cyber security that seeks to address the emerging cyber terrorist threat.

This chapter is divided into six different parts. In the first part, NATO's cyber defence policy from post-Cold War to 2010 will be explained and analysed. More details will be given about the process of NATO's policy, and some examples, comprehensive plans, and Summit Declarations will be briefly discussed in the first section of the chapter. In the second section, NATO's current cyber policy will be analysed and clarified under the Summit Declarations, experts' documents and Strategic Concept, in order to understand NATO's newly revised policy in terms of the effect of cyber threats.

In the third part of the chapter, the application of Game Theory to NATO's cyber defence policy will be examined, analysed and clarified. Because NATO has found it difficult to respond to new threat perceptions in a timely and flexible manner, I suggest that Game Theory is a possible way to reveal how a strategy could be bought in by senior NATO officials to address their willingness to acknowledge new realities with a strategic concept.

In the fourth part of the chapter, the evaluation of NATO's policy in the context of international law will be analysed and clarified. In this section, Articles 4 and 5 of the North Atlantic Treaty will be mentioned, and the policy and international law will be compared, and NATO's policy will be explained under international law in order to understand these two things together.

In the fifth part of the chapter, the research will be reviewed and some recommendations offered. NATO's policy will be criticised in this part, in order to learn more about its negative consequences, and some recommendations will be given for an effective cyber security policy.

The policy will be evaluated and the research will be concluded in the final part of the chapter. First-hand sources, Internet sources, books and articles will be used to understand and analyse NATO's policy in detail.

5.2. NATO‘s Cyber Defence Policy from Post-Cold War to 2010

5.2.1. The Evaluation of NATO's Cyber Policy from the First Cyber Attack to NATO

Following the end of the Cold War, NATO's new security policy was developed in the London Summit in 1990. According to the resolution of the Declaration, *"...in the new Europe, the security of every state is inseparably linked to the security of its neighbours. NATO must become an institution where Europeans, Canadians and Americans work* *together not only for the common defence, but to build new partnerships with all the nations of Europe.*"[755]

NATO's first post-Cold War Strategic Concept was adopted in 1991. The Concept highlighted a reduction of the threat from the Soviet Union and identified "*serious economic, social and political difficulties, including ethnic rivalries and territorial disputes, which are faced by many countries in central and Eastern Europe"*[756], adding that "*NATO must be capable of responding to such risks if stability in Europe and the security of Alliance members are to be preserved. These risks can arise in various ways*."[757] Due to the changing the nature of the concept of threat that of risk, NATO used the concept of risk to adapt itself to the new era. As detailed in Chapter 2, in the Cold War era, the threat was regarded as the Soviet Union towards the Western Block, and the USA towards the Eastern Block. However, risks and uncertainties are harder to define, and can come from anywhere. Therefore NATO has used the concept of risk to identify its new role in the international arena.

This strategy was tested by the Kosovo War between 1998-1999, which forced NATO to consider new attack strategies. On 30th January, 1999, the North Atlantic Council released a statement on Kosovo that stated, "*The Council has therefore agreed today that the NATO Secretary General may authorise air strikes against targets on FRY territory."*[758] On 24th March, 1999, following the announcement of a strike against the Serb targets by the General Secretary, the first cyber-attacks were launched against NATO.[759] With these cyber-attacks, NATO's cyber story had begun.

The main aim of the Serbian attackers was to demonstrate their reaction against the Allies because of the authorisation of air strikes against their territories. The attackers mostly used Distributed Denial of Service (DDoS)[760] attacks against NATO to block its operation

[755] NATO (1990), *London Declaration on a Transformed North Atlantic Alliance*, Available at: http://www.nato.int/docu/comm/49-95/c900706a.htm (Accessed at: 15/08/2012)

[756] NATO (1991), *The Alliance's New Strategic Concept*, 7 November, Available at: http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Accessed at: 10/04/2014)

[757] *Ibid*.

[758] NATO (1999), *Statement by the North Atlantic Council on Kosovo*, 30 January, Available at: http://www.nato.int/docu/pr/1999/p99-012e.htm (Accessed at: 25/09/2013), Also see, Healey, J. and Bochoven, L.V. (2012), "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council Issue*, February 2012, p.1

[759] Theiler, O. (2011), *New Threats: The Cyber Dimension*, Available at: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (Accessed at: 01/02/2012)

[760] DDOS is defined as a situation where, "a malicious hacker uses a DDOS attack to make a computer resource (i.e. website, application, e-mail, voicemail, network) stop responding to legitimate users. The malicious hacker does this by commanding a fleet of remotely-controlled computers to send a flood of network traffic to the target. The target becomes so busy dealing with the attacker's requests that it does not have time to respond to legitimate users' requests. That can cause the target system to respond, resulting in long delays and outages." "The definition of DDOS", Available at: http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html (Accessed at: 01/07/2014)

centre.[761] Venkantesh explains these attacks as "*DDOS attacks employ armies of zombie machines taken over and controlled by a single master to overwhelm the resources of victims with flood of packets*".[762] According to Klimburg, "*As these attacks were relatively minor they were primarily an issue for the 'counter cybercrime mandate' of NCS, and not one for 'collective defence', no matter how interpreted. ... Despite the severity of those attacks, it was not considered to have actually crossed the line where military collective defence would be necessary. As with the 1999 incident, the 'military mandate' did not come to the fore, although nations did provide technical and policing assistance relevant to other mandates*."[763] Whilst NATO sought to evaluate them as cybercrimes, I suggest that another way of looking at this attack is to argue that the Serbian attackers had used a form of asymmetric conflict which defined as, "*warfare in which opposing groups or nations have unequal military resource, and the weaker opponent uses unconventional weapons and tactics, as terrorism, to exploit the vulnerabilities of the enemy*."[764] Perhaps because of the evaluation of the Serbian attacks as cybercrime, NATO's 1999 Strategic Concept did not directly address cyber threats.

In 1999, the Alliance's new Strategic Concept was published recognising that threat perceptions had changed following the end of the Cold War. In the document NATO identified:

> *"The appearance of complex new risks to Euro-Atlantic peace and stability, including oppression, ethnic conflict, economic distress, the collapse of political order, and the proliferation of weapons of mass destruction."*[765]

The Strategic Concept identified the following as risks: terrorism, human rights abuses, political instability and organized crime,[766] and observed that:

[761] Bıçakçı, S. (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler*, Cilt 9 Sayı 34, Available at: http://www.academia.edu/1828068/The_Rebirth_of_NATO_between_New_War_and_Cyber_Security (Accessed at: 13/06/2012), p. 210. Healey and Bochoven, *Ibid.*

[762] Venkantesh, S. (2003), *Cyber Terrorism*, Delhi: Authors Press, p. 128

[763] Klimburg, A. (ed.) (2012), *National Cyber Security Framework Manual*, Tallinn: NATO CCDCOE Publications, Available at: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Accessed at: 05/09/2013), p.182. Healey and Bochoven, *Ibid.*

[764] "The definition of Asymmetric Warfare", Available at: http://dictionary.reference.com/browse/asymmetric+warfare (Accessed at: 01/07/2014)

[765] NATO (1999), *The Alliance's Strategic Concept*, 24 April, Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Accessed at: 15/04/2012)

[766] *Ibid.*

> "*The maintenance of the security and stability of the Euro-Atlantic area is of key importance. An important aim of the Alliance and its forces is to keep risks at a distance by dealing with potential crises at an early stage. In the event of crises which jeopardise Euro-Atlantic stability and could affect the security of Alliance members, the Alliance's military forces may be called upon to conduct crisis response operations. They may also be called upon to contribute to the preservation of international peace and security by conducting operations in support of other international organisations, complementing and reinforcing political actions within a broad approach to security.*"[767]

With the new concept, NATO sought to improve its capability to respond to international crisis as well as recognising that:

> *"The global spread of technology that can be of use in the production of weapons may result in the greater availability of sophisticated military capabilities, permitting adversaries to acquire highly capable offensive and defensive air, land, and sea-borne systems, cruise missiles, and other advanced weaponry. In addition, state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems. They may attempt to use strategies of this kind to counter NATO's superiority in traditional weaponry."*[768]

The importance of the Strategic Concept 1999 is the legality of off-site operations, provided by Article 5 of the NATO Treaty, thereby giving the authority for NATO to conduct military operations outside its boundaries.

NATO began to adopt cyber security policies following the Prague Summit of 2002, suggesting that the Allies had finally awakened to the danger of cyber-attacks.

5.2.2. The First Step towards Cyber Policy of NATO

The development of technology has created new risks and threats to the international community. As it is states above that NATO experienced its first cyber-attack during the Kosovo war, and therefore NATO has decided to improve its cyber security. The Prague Summit 2002 was the first time that cyber security was placed on the political agenda of the

[767] *Ibid*.

[768] *Ibid*.

Alliance.[769] The Allies decided to strengthen their capabilities to defend against cyber-attacks[770] A Cyber Defence Programme was approved and a three stage comprehensive plan accepted. The main aim was to improve the Alliance's cyber capability. For this reason, the NATO Computer Incident Response Capability (NCIRC) was established.[771] A European Parliament document, the *Defending against Cyber Attacks* was mentioned this comprehensive plan as:

> 1) *The first phase covered the creation of the currently functioning NCIRC establishing its interim operating capability;*
> 2) *The second phase will make most NCIRC capabilities fully operational by 2012;*
> 3) *The third phase identifies requirements and resources to eliminate or mitigate other vulnerabilities. This initiative broadens the cyber defence view for inclusion of CDMA capabilities and the identification of "Enterprise-wide solutions" and demonstrates how new technologies could be exploited to reduce the risks associated with cyber-attacks.*[772]

According to Healey and Bochoven, "*The most important element of the Program was creation of the NATO Computer Incident Response Capability (NCIRC), the Alliance's 'first responders' to prevent, detect, and respond to cyber incidents*."[773] With the development of

[769] Noshiravani, R. (2011), "NATO and Cyber Security: Building on the Strategic Concept", *Rapporteur Report*, Available at: http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/200511nato.pdf (Accessed at: 05/08/2012), p.4. Also see, "NATO and Cyber Defence" (2013), Available at: http://www.nato.int/cps/en/natolive/topics_78170.htm (Accessed at: 13/08/2013). Healey and Bochoven, *op.cit.*, p.1. Efthymiopoulos, M. P. (2010), *Challenging NATO's Security Operations in Electronic Warfare: The Policy of Cyber-Defence: the Case of Greece,* Available at: http://www.lse.ac.uk/europeanInstitute/research/hellenicObservatory/pdf/4th_%20Symposium/PAPERS_PPS/FOREIGN_SECURITY_POLICY/EFTHYMIOPOULOS.pdf (Accessed at: 08/04/2012), p.5. and "The Prague Summit and NATO's Transformation", (2003), Available at: http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf (Accessed at: 03/02/2012)

[770] NATO (2002), *Prague Summit Declaration*, Available at: http://www.nato.int/docu/pr/2002/p02-127e.htm (Accessed at: 01/06/2012)

[771] "Defending Against Cyber Attacks", Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf (Accessed at: 07/08/2013). NATO (2011), *Bilgilendirme*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf (Accessed at: 08/05/2013), p.9. Hunker, J. (2013), "NATO and Cyber Security", in Herd, G. P. and Kriendler, J. (eds.) (2013), *Understanding NATO in the 21st Century,* Oxon: Routledge, p.157

[772] "Defending Against Cyber Attacks", *Ibid.*, Also see, Efthymiopoulos, *op.cit.*, and "NATO and Cyber Defence", Available at: http://www.nato.int/issues/cyber_defence/practice.html (Accessed at: 05/07/2013)

[773] Healey and Bochoven , *op.cit* .p.2

the NCIRC[774] [775], NATO started to respond to cyber threats, showing concern about the threats of cyberspace.

The Prague Summit of 2002 was a milestone in changing the perception of cyber security and the logic of strategy. The Summit signalled that NATO was prepared to take important initiatives to defend its information infrastructure and began to create institutions that would have a major role in achieving this in the future. The NATO Network Enabled Capability was started after the Summit, the main aim being to combine the military and civilian elements of NATO's information infrastructure.[776] The need to protect the information infrastructure was further emphasised in the Riga Summit of 2006:[777]

> *"...work to develop a NATO Network Enabled Capability[778] to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber-attack."*[779]

After the attacks against Estonia, NATO started to take new steps against cyber threats.[780] Prior to the cyber-attacks against Estonia, NATO's cyber policy only covered its own cyber security, but after the attack, the plan was expanded to include and strengthen its Allies' information systems.[781] According to Theiler, "*The Alliance therefore drew up for the first time ever a formal 'NATO Policy on Cyber Defence', adopted in January 2008, that established three core pillars of Alliance cyberspace policy:*

> ***Subsidiarity****, i.e. assistance is provided only upon request; otherwise, the principle of sovereign states' own responsibility applies;*

[774] The NCIRC's role has been explained as: "NCIRC has a key role in responding to any cyber aggression against the Alliance. It provides a means for handling and reporting incidents and disseminating important incident-related information to system/ security management and users. It also concentrates incident handling into one centralized and coordinated effort, thereby eliminating duplication of effort." "Defending Against Cyber Attacks", *op.cit.*

[775] NATO explains the role of the NCIRC as:
"The NCI Agency, through its NATO Computer Incident Response Capability (NCIRC) Technical Centre, is responsible for the provision of technical and operational cyber security services throughout NATO. NCIRC is a two-tier functional capability where the NCIRC Technical Centre constitutes NATO's principal technical and operational capability and has a key role in responding to any cyber aggression against the Alliance." "NATO and Cyber Defence" (2013), *op.cit*

[776] Bıçakçı (2012), *op.cit.*, pp. 212-213

[777] *Ibid*.. Efthymiopoulos, *op.cit*.

[778] For more information, "NATO Network Enabled Capability" (2010), Available at: http://www.nato.int/cps/de/SID-815535E4-57782C82/natolive/topics_54644.htm (Accessed at: 08/06/2012)

[779] NATO (2006), *Riga Summit Declaration*, Available at: http://www.nato.int/docu/pr/2006/p06-150e.htm (Accessed at: 04/05/2012)

[780]Noshiravani , *Ibid*.

[781] NATO (2011), *Bilgilendirme*, *op.cit*., pp.7-9. And Noshiravani , *Ibid*. and NATO Parliamentary Assembly (2009), *op.cit.*

> ***Non-duplication**, i.e. avoiding unnecessary duplication of structures or capabilities – at international, regional, and national levels; and*
>
> ***Security**, i.e. cooperation based on trust, taking into account the sensitivity of the system-related information that must be made accessible and possible vulnerabilities."*[782]

A little information must be given here about the North Atlantic Council (NAC). Briefly the NAC is the principal political decision-making body within NATO with a central and final decision-making role on cyber defence, together with other political decisions. It brings together high-level representatives of each member country to discuss policy or operational questions requiring collective decisions. In sum, it provides a forum for wide-ranging consultation between members on all issues affecting their peace and security. The NAC was established under Article 9[783] of the North Atlantic Treaty[784] it evaluates NATO's policies and activities in political and military terms. Over the years, NAC-UN cooperation includes consultations between NATO and UN on issues such as crisis assessment and management, civil-military cooperation, training and education, logistics, combating human trafficking, mine action, civilian capabilities, women, peace and security, arms control and non-proliferation, and the fight against terrorism.

Another important development took place during the Riga Summit in 2006. NATO endorsed the Comprehensive Political Guidance during the Summit, and according to this Guidance, agreed to protect information systems against cyber-attacks.[785]

5.2.3. New Approaches to a Common Cyber Policy

5.2.3.1.The Bucharest Summit in 2008

NATO produced new policies to protect itself and its Allies against cyber threats following the Prague Summit of 2002 and reviewed its own cyber defence systems after the cyber-attacks on Estonia.[786] Following the cyber-attacks on Estonia, NATO broadened its focus on

[782] Theiler, *op.cit.*

[783] Article 9 of the North Atlantic Treaty: "The Parties hereby establish a Council, on which each of them shall be represented, to consider matters concerning the implementation of this Treaty. The Council shall be so organised as to be able to meet promptly at any time. The Council shall set up such subsidiary bodies as may be necessary; in particular it shall establish immediately a defence committee which shall recommend measures for the implementation of Articles 3 and 5."

[784] Thessismun 2014 (2014), *Guide for Comminuque Drafting of the North Atlantic Council (NATO)*, Available at: http://thessismun.org/2014/wp-content/uploads/2012/11/Communique-2014.pdf (Accessed at: 16/09/2014)

[785] NATO (2006), *Comprehensive Political Guidance*, Available at: http://www.nato.int/cps/en/natolive/official_texts_56425.htm (Accessed at: 12/10/2016)

[786] NATO (2011), *Bilgilendirme*, *op.cit.*, Cavelty (2011), *op.cit.*

cyber threats.[787] Following the attacks, a report, *Defending Against Cyber Attacks* was prepared to submit to Ministers of the Allies. This recommended certain measures for implementation to protect themselves and NATO from any cyber-attack.[788]The report also covered the development of NATO's cyber policy.[789] The development of new policy on cyber threats was comprehensively discussed at the Bucharest Summit of 2008, and more detailed decisions were stated in the Summit Declaration.[790]

> "*NATO remains committed to strengthening key Alliance information systems against cyber-attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber-attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities."*[791]

The development of NATO's cyber defence policy was approved in January 2008, and accepted by the leaders of NATO at the Bucharest Summit in 2008.[792] This situation of the new cyber defence policy may cause some confusion to readers, and so it is necessary to explain it here. NATO has been protecting its cyber defence since the problem was identified as a threat, but initially the policy was not interpreted broadly, in other words NATO determined new policies in reaction to the threats they perceived at the time. For instance, NATO accepted a cyber-defence programme in the Prague Summit of 2002, the plan covering one specific aim, which was the establishment and improvement of NCIRC[793]. This institution was thus established and improved by the Allies, who supplied economic

[787] "Defending Against Cyber Attacks", *op.cit.*
[788] *Ibid.*
[789] NATO Parliamentary Assembly (2009), *op.cit.*
[790] Bıçakçı (2012), *op.cit.*, p.217. Also see, Hughes, R. B. (2009), *NATO and Cyber Defence: Mission Accomplished,* Available at: http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf (Accessed at: 05/07/2012), p.1
[791] NATO (2008), *Bucharest Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_8443.htm (Accessed at: 02/01/2012)
[792] NATO Parliamentary Assembly, *op.cit.*
[793] As mentioned previously, the plan was comprehensive and the main aim was to improve the ability of NATO with the creation of NCIRC. Therefore, the researcher explains it in here on NCIRC.

investment to it.[794] Furthermore, the Allies produced new strategies in Riga (2006) and Bucharest (2008), but the first time the cyber policy was broadly discussed and decisions taken was in Bucharest in 2008.

Following the Bucharest Summit of 2008, there have been two important developments in the cyber security policy of NATO. Firstly, the Cyber Defence Management Authority (CDMA), or Cyber Defence Management Board (CDMB)[795] was established, and secondly, the Cooperative Cyber Defence Centre of Excellence[796] (CCD COE)[797] was accredited by NATO in 2008.[798]

5.2.3.2.Cyber Defence Management Board (CDMB)

As with the other organs of NATO, the CDMB has a particular role, which Hunker explains: "*… maintains sole responsibility for coordinating cyber defence across the Alliance*."[799] NATO describes its role as having, "*responsibility for coordinating cyber defence throughout NATO civilian and military bodies. The NATO CDMB comprises the leaders of the political, military, operational and technical staffs in NATO with responsibilities for cyber defence*."[800] NATO's aim was to establish and accredit bodies, such as NCIRC, CDMB and CCDCOE to create and coordinate new policies to combat cyber threats. Healey and Bochoven identify CDMB's duties as including the provision of help to member states to improve their national cyber capabilities.[801] As well as providing help to member states, CDMB also has the sole role to coordinate NATO bodies. The NATO Parliamentary Assembly states that "*The*

[794] Paganini, P. (2013), *NATO Has Constituted Cyber Response Teams,* Available at: http://securityaffairs.co/wordpress/20705/cyber-warfare-2/nato-attack-response-teams.html (Accessed at: 16/09/2014)

[795] CDMA is replaced by CDMB. After this CDMB will be used.

[796] The organisation was set up in 2003.

[797] More Information, "NATO Cooperative Cyber Defence Centre of Excellence", Available at: http://www.ccdcoe.org/ (Accessed at: 05/04/2011)

[798] "NATO Agrees Common Approach to Cyber Defence" (2012), Available at: http://www.euractiv.com/infosociety/nato-agrees-common-approach-cyber-defence/article-171377 (Accessed at: 05/06/2013) and see**,** NATO (2011), *Bilgilendirme, op.cit.*. Mcgee, J. (2011), "NATO and Cyber Defense: A Brief Overview and Recent Events' exercises", *Centre for Strategic and International Studies,* Available at: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events (Accessed at: 03/09/2014)

[799] Hunker, J. (2010), "Cyber War and Cyber Power: Issues for NATO Doctrine", *NATO Defence College*, No 62, Available at: http://www.ndc.nato.int/research/series.php?icode=1 (Accessed at: 08/03/2012), p.8. And see O'Connell, M. E. (2012), "Cyber Security without Cyber War", Journal of Conflict and Security Law, Summer, Vol. 17(2), Available at: http://jcsl.oxfordjournals.org/content/17/2/187.full#fn-46 (Accessed at: 06/02/2013), pp.195-196

[800] "NATO and Cyber Defence" (2013), *op.cit.*

[801] Healey and Bochoven, *op.cit*. p.2

CDMA (CDMB) is unique in its structure because it consolidates the management of all of these tasks and agencies under a body with permanent political-level representation."[802]

5.2.3.3. Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Estonia proposed the concept of the CCDCOE in 2004 after joining NATO, and it was approved in the Riga Summit of 2006.[803] The organisation was fully accredited by NATO in 2008, after the resolution of the Bucharest Summit.

The CCDCOE explains its mission as "*(enhancing) the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.*"[804] Also, the NATO Parliamentary Assembly states its role as:

> "[CCDCOE was] *set up as a primary source of expertise for NATO in co-operative cyber defence related matters, the main tasks of the 30-person body include:*
>
> *1) Providing cyber-related doctrines and concepts for the Alliance;*
>
> *2) Hosting and conducting training workshops, courses, and exercises for NATO member states;*
>
> *3) Conducting research and development activities;*
>
> *4) Studying past or ongoing attacks to draw up lessons learned; and*
>
> *5) Providing advice, if asked, during ongoing attacks.*"[805]

The CCDCOE main aim is to produce new ideas on cyber security, and exercise these policies with activities dealing with the long-term cyber capability of NATO and its Allies.[806] [807]

[802] NATO Parliamentary Assembly (2009), *op.cit.*

[803] NATO Cooperative Cyber Defence Centre of Excellence (2015), *History*, Available at: http://www.ccdcoe.org/history.html (Accessed at: 10/08/2014)

[804] NATO Cooperative Cyber Defence Centre of Excellence (2013), *Mission and Vision*, Available at: https://www.ccdcoe.org/11.html (Accessed at: 06/08/2013)

[805] NATO Parliamentary Assembly, *op.cit.* and Bıçakcı, *op.cit.*, p. 218

[806] Hughes (2009), *op.cit.*

[807] In accordance with this, some exercises have been conducted since 2010, such as Baltic Cyber Shield 2010, Locked Shields 2012, Locked Shields 2013 and Locked Shields 2014. For more details about the exercises; NATO Cooperative Cyber Defence Centre of Excellence (2010), *Baltic Cyber Shield 2010*, Available at: http://www.ccdcoe.org/baltic-cyber-shield-2010.html (Accessed at: 11/08/2014). NATO Cooperative Cyber Defence Centre of Excellence (2012), *Locked Shields 2012*, Available at: http://www.ccdcoe.org/locked-shields-2012.html (Accessed at: 11/08/2014). NATO Cooperative Cyber Defence Centre of Excellence (2013), *Locked Shields 2013*, Available at: http://www.ccdcoe.org/locked-shields-2013.html (Accessed at: 11/08/2014). NATO Cooperative Cyber Defence Centre of Excellence (2014), *Locked Shields 2014*, Available at: http://www.ccdcoe.org/locked-shields-2014.html (Accessed at: 11/08/2014)

5.2.3.4.The Strasburg/Kehl Summit in 2009

The Strasburg/Kehl Summit Declaration in 2009 provides that:

> "*We remain committed to strengthening communication and information systems that are of critical importance to the Alliance against cyber-attacks, as state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems. To prevent and respond to such attacks, in line with our agreed Policy on Cyber Defence, we have established a NATO Cyber Defence Management Authority, improved the existing Computer Incident Response Capability, and activated the Cooperative Cyber Defence Centre of Excellence in Estonia. We will accelerate our cyber defence capabilities in order to achieve full readiness. Cyber defence is being made an integral part of NATO exercises. We are further strengthening the linkages between NATO and Partner countries on protection against cyber-attacks. In this vein, we have developed a framework for cooperation on cyber defence between NATO and Partner countries, and acknowledge the need to cooperate with international organisations, as appropriate.*"[808]

The importance of the declaration of the Strasburg/Kehl Summit is that the cyber defence programme became an essential part of exercises conducted by NATO where experts tried to find new ways to provide protection against cyber-attacks.

5.3. NATO's Cyber Policy Today

5.3.1. NATO 2020: Assured Security, Dynamic Engagement

After the Strasburg/Kehl Summit in 2009, a group of experts was brought together under the leadership of Anders Fogh Rasmussen, Secretary General of NATO, to define new threats and recommend new strategies to the Alliance.[809] The main aim was to prepare a report advising "*NATO on the way it should strategically go forward during the next ten years.*"[810]

[808] NATO (2009), *Strasbourg/Kehl Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease (Accessed at: 21/07/2013)

[809] McMahon, R. J. and Zeiler, T. W. (Eds.) (2012), *U.S. Foreign Policy: A Diplomatic History*, London: CQ Press, p. 498

[810] Anil, S. (2010), "Cyber Security in NATO 2002 to 2020", in Deloitte (2010), "Cyber Security for Government CIO's", *Deloitte 1st European Cyber Security*, Available at: http://www.deloitte.com/assets/Dcom-Namibia/Local%20Assets/Documents/cyber%20security%20round%20table%20report_final.pdf (Accessed at: 05/03/2013), p.8

The report *NATO 2020: Assured Security; Dynamic Engagement* was submitted to NATO in May 2010. Three main threats were identified:[811]

> "*1) an attack by a ballistic missile (whether nuclear armed or not);*
> *2) strikes by international terrorist groups; and*
> *3) cyber assaults of varying degrees of severity.*"[812]

The report recommended the following for NATO:

> *"The danger posed by unconventional threats has obvious implications for NATO preparedness, including its definition of security, its strategies for deterrence, its need for military transformation, its ability to make decisions rapidly, and its reliance for help on countries and organisations from outside the Alliance."*[813]

Another of the other recommendations is that:

> *"NATO must accelerate efforts to respond to the dangers of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."*[814]

The report stated, "*However, the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5.*"[815] This suggests that, cyber threats can engage Articles 4 and 5 of the North Atlantic Treaty, and, therefore, these attacks can be evaluated under the collective security of NATO. This conclusion is supported by the Report:

> "*These dangers include attacks involving weapons of mass destruction, terrorist strikes, and efforts to harm society through cyber assaults or the unlawful disruption of critical supply lines. To guard against these threats, which may or may not reach the level of an Article 5 attack, NATO must update its approach to the defence of Alliance territory while also*

[811] *Ibid*.
[812] Group of Experts Report (2010), *NATO 2020: Assured Security; Dynamic Engagement*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf (Accessed at: 10/04/2012), p.17
[813] *Ibid.*
[814] *Ibid*, p.11
[815] *Ibid*., p.45

> *enhancing its ability to prevail in military operations and broader security missions beyond its borders*."[816]

The Report clearly suggests re-defining the North Atlantic Treaty Articles, in particular Articles 4 and 5, because of the changing threat perceptions.[817]

Although NATO has taken steps to prevent cyber-attacks, the group of experts drew attention to serious gaps in its cyber defence capabilities offering the following recommendations:

> *"NATO should recognize that cyber-attacks are a growing threat to the security of the Alliance and its members. Accordingly:*
>
> 1) *A major effort should be undertaken to increase the monitoring of NATO's critical network and to assess and furnish remedies to any vulnerabilities that are identified.*
> 2) *The Centre of Excellence should do more, through training, to help members improve their cyber defence programmes.*
> 3) *Allies should expand early warning capabilities in the form of a NATO-wide network of monitoring nodes and sensors.*
> 4) *The Alliance should be prepared to send an expert team to any member experiencing or threatened by a major cyber-attack.*
> 5) *Over time, NATO should plan to mount a fully adequate array of cyber defence capabilities, including passive and active elements."*[818]

The report is important in terms of the effect of the new Strategic Concept of 2010, because the new threat perceptions demand new policies and plans for cyber security.

5.3.2. Lisbon Summit in 2010

Whilst previous Summit declarations identified cyber threats, in the Lisbon Summit 2010, cyber policy was expressly written into the language of the NATO's Strategic Concept.[819]

5.3.3. Active Management and Modern Defence (Strategic Concept)

NATO's new Strategic Concept, was accepted in November 2010. It identified that active engagement and modern defence was needed:

[816] *Ibid*., p.8

[817] Since the establishment of NATO, it has only applied Article 5 in 2001, after the terrorist attack of 9/11.

[818] *Ibid*., p.45

[819] NATO (2011), *Bilgilendirme*, *op.cit*., p.8. Hunker, (2010), *op.cit.*

> "*12. Cyber-attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies, and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Foreign militaries and intelligence services, organized criminals, terrorist, and/or extremist groups can each be the source of such attacks.*
>
> *13. All countries are increasingly reliant on the vital communication, transport and transit routes on which international trade, energy security and prosperity depend. They require greater international efforts to ensure their resilience against attack or disruption."*[820]

According to Klimburg, "*To tackle these challenges, NATO endorsed the 'in-depth cyber defence' concept at the Lisbon Summit 2010,*[821] *a strategy which cuts across a variety of stakeholders and implicitly embraces the Whole of Government approach, due to the fact that the lead responsibility of cyber defence in most nations resides in civilian agencies and with non-governmental actors. In 2010, NATO presented its latest Strategic Concept which recognised the growing international significance of cyber security, both as an issue for NATO to address in terms of capability, and as a challenge in respect of NATO's future international relevance."*[822] With the new Strategic Concept, NATO has tried to encourage its members to take urgent steps to stop cyber-attacks. The concept also highlighted the need to "*develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.*"[823]

The new Strategic Concept also uses the concept of threat and security challenges rather than the concept of risk. The document states that "*this Strategic Concept will guide the next phase in NATO's evolution, so that it continues to be effective in a changing world, against new threats, with new capabilities and new partners*."[824] According to Flockhart, this

[820] NATO (2010), "Active Engagement, Modern Defence", *Strategic Concept*, Available at: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (Accessed at: 04/06/2013)

[821] NATO (2010), *Lisbon Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease (Accessed at: 04/06/2013)

[822] Klimburg, *op.cit.*, p.181., and *Ibid*.

[823] NATO (2010), "Active Engagement, Modern Defence", *op.cit.*, p.16

[824] Heads of State and Government (2010), *Active Engagement, Modern Defence*, Available at: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (Accessed at: 24/08/2016)

strategic concept was innovative, because the document clearly states the identities and core tasks of NATO.[825] The core tasks are mentioned in the document as: collective defence, crisis management and cooperative security. It is clear that NATO has improved post-Cold War strategy, which is collective defence with a new Strategic concept.

5.3.4. The New Revised Cyber Policy of NATO

The members of the Alliance Defence Ministers drafted the NATO concept on cyber defence policy, defending NATO systems in March 2011, and it was accepted in June 2011.[826] After the Riga Summit of 2006, NATO accepted a plan to help and strengthen its Allies' information systems against cyber-attacks. The new policy stated that the protection of the Alliance's cyber systems was the responsibility of the members, rather than NATO.[827] The revised 2011 policy provided that NATO will help members or states if requested providing that:

> "*NATO cyber defence efforts are based on the overarching principles of* ***prevention and resilience and non-duplication****. Prevention and resilience are particularly important given the reality that certain threats will persist despite all efforts to protect and defend against them. Preventing such attacks from occurring in the first place will be achieved by increasing our level of preparedness and mitigating risk by limiting disruptions and their consequences. Resilience is the key because it facilitates rapid recovery in the aftermath of an attack."*[828]

The focus on resilience means that this policy points to NATO accepting the serious impact of cyber-attacks and the power of cyber terrorists. I would further suggest that "*mitigating risk by limiting disruptions and their consequences"* implies that the cyber terrorists have more information than the NATO experts. This suggests to a worrying admission that NATO may not guarantee protection against any cyber-attack. For example if attacks target recovery systems[829], NATO might be powerless to respond against any cyber-attack if the recovery

[825] Flockhart, T. (2016), "Understanding NATO Through Constructivist Theorising", in Webber, M. and Hyde-Price, A. (2016), *Theorising NATO: New Perspectives on the Atlantic Alliance*, London: Routledge, p. 154

[826] Klimburg, *op.cit*., p. 181. Also see, NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (Accessed at: 04/09/2013)

[827] Klimburg, *Ibid*., p. 181

[828] NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence*, *op.cit.*

[829] Recovery system is defined by Business Dictionary as, "*rebuilding a computer system after a disaster so that its operating system and other software may be reinstalled*". Business Recovery, "System Recovery", Available at: http://www.businessdictionary.com/definition/system-recovery.html (Accessed at: 09/12/2015)

systems of NATO have any problem after the cyber-attacks, and therefore NATO may not response to solve the problem and the information infrastructure will be damaged. This question might be answered in the future, if NATO develops an alternative plan to recover its own systems.

Hunker, writing of the new policy, indicates "*the NATO Policy on Cyber Defence and the accompanying Action Plan*[830] *make clear that NATO's focus is on the protection of its own communication and information systems. The underlying policy principles are based on prevention, resilience, and non-duplication. Certain threats will persist despite all efforts to eliminate them. Prevention is about mitigating risk. Resilience is about facilitating rapid recovery after an attack."*[831] Also, Anıl mentions that the new policy is based on the protection of NATO's own systems from attack, but that if there is a request from any members to protect their cyber systems, NATO will help to improve the members' cyber system capabilities.[832]

After the Lisbon Summit, cyber defence began to be integrated into the NATO Defence Planning Process (NDPP)[833] in April 2012.[834] The NDPP has the sole responsibility of guiding the integration of cyber defence into national defence structures. The policy states that "*the NATO Defence Planning Process (NDPP) will guide the integration of cyber defence into national defence frameworks. Recognising that NATO requires a secure infrastructure upon which it can operate, NATO networks, including NATO agencies and NATO missions abroad, will be brought under centralised protection. NATO will also develop minimum requirements for those national networks that are connected to or process NATO information.*"[835] Also, this policy is important to improve cyber security policies of states, but the problem is that the technology is not standard and today's rules cannot be used tomorrow, and NATO and its members should add new requirements to improve their cyber security policies.

The main elements of the new revised cyber policy are to:

> *"1) Integrate cyber defence considerations into NATO structures and planning processes in order to perform NATO's core tasks of collective defence and crisis management.*

[830] *Ibid*.
[831] Hunker, J. (2013), *op.cit*., p. 159
[832] Anil, *op.cit*., p.8. NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence*, *op.cit.*
[833] More Details about the NDPP: Klimburg, *op.cit*., p.187 and NATO (2014), *The NATO Defence Planning Process*, Available at: http://www.nato.int/cps/en/natolive/topics_49202.htm (Accessed at: 15/08/2014)
[834] NATO (2014), *Ibid*.
[835] *Ibid*.

2) Focus on prevention, resilience and defence of critical cyber assets to NATO and Allies.

3) Develop robust cyber defence capabilities and centralise protection of NATO's own networks.

4) Develop minimum requirements for cyber defence of national networks critical to NATO's core tasks.

5) Provide assistance to the Allies to achieve a minimum level of cyber defence and reduce vulnerabilities of national critical infrastructures.

6) Engage with partners, international organisations, the private sector and academia."[836]

With the new policy, the NATO Cyber Defence Management Board signed a Memorandum of Understanding with each member of NATO.

NATO has started to take serious steps to guard against cyber-attacks with the acceptance of new strategic concept and new cyber defence policy. Significantly their cyber defence policy allows cooperation with other organisations, partners, the private sector and academia to improve its capability.

NATO prepared practical steps to implement the policy as follows:

1) NATO will develop minimum requirements for those national information systems that are critical for carrying out NATO's core tasks.

2) NATO assists Allies in achieving a minimum level of cyber defence in order to reduce vulnerabilities to national critical infrastructure.

3) Allies can also offer their help to an Ally or to the Alliance in case of a cyber-attack.

4) Cyber defence will be fully integrated into the NATO Defence Panning Process. Relevant cyber defence requirements will be identified and prioritised through the NDPP.

5) NATO Military Authorities will assess how cyber defence supports performing NATO's core tasks, planning for military missions, and carrying out missions.

6) Cyber defence requirements for non-NATO troop contributing nations will also be defined.

[836] *Ibid.*

7) Strong authentication requirements will be applied. The acquisition process and supply chain risk management requirements will be streamlined.

8) NATO will enhance early warning, situational awareness, and analysis capabilities.

9) NATO will develop awareness programs and further develop the cyber component in NATO exercises.

10) NATO and Allies are encouraged to draw on expertise and support from the Cooperative Cyber Defence Centre of Excellence in Tallinn."[837]

It can be seen here that NATO has attempted to resolve cyber threats with this policy, and the duty has been enlarged to cover all bodies of NATO and its members.

5.3.4.1.Rapid Reaction Teams

The Rapid Reaction Team or Force's capability has been developed, and new initiatives added to the Force to extend its capability regarding cyber threats.[838] Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges at NATO explains why this is compulsory: "*The number of cyber-attacks is rising every day, whether they be against NATO systems or against the vital systems of our member nations. NATO must be able to offer cyber defence assistance to its members to help them guard against these attacks, to detect them, and - once they have happened - to react swiftly to limit the damage.*"[839] Following the new revised policy in 2011, NATO has started to endorse Rapid Reaction Teams. Alex Vandurme, head of the engineering section of the NCIRC, explains the Rapid Reactions Team purpose as: "*[responsibility] for assisting member states which ask for help in the event of an attack of national significance.*"[840] Bıçakçı also mentions that the aim of the Force is to help the members of NATO when needed.[841] The NATO Rapid Reaction programme was fully

[837] NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence*, *op.cit.*

[838] Belkin, P., Ek. C., Mages, L. and Mix, D. E. (2009), "NATO's 60th Anniversary Summit", *Congressional Research Service,* Available at: http://www.fas.org/sgp/crs/row/R40454.pdf (Accessed at: 06/05/2013), p.13. NATO Parliamentary Assembly, *op.cit*. and Palmer, D. R. (2009), "From AMF to NRF", *NATO Review*, Available at: http://www.nato.int/docu/review/2009/0902/090204/EN/index.htm (Accessed at: 08/03/2013) and The European Parliament (2011), *Defending Against Cyber Attacks*, Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611natocyberattacks_/sede150611natocyberattacks_en.pdf (Accessed at: 02/04/2012)

[839] NATO (2012), *NATO Rapid Reactions Team to Fight Cyber Attack*, Available at: http://www.nato.int/cps/en/natolive/news_85161.htm (Accessed at: 08/07/2014)

[840] *Ibid*.

[841] Bıçakçı (2012), *op.cit.*, pp. 221-222

operational[842] by the end of 2012,[843] and, according to Alex Vandurme, the Rapid Reaction Team will respond to any attack within 24 hours of the incident.[844] Although mentioned in the Chicago Summit of 2012, and having 58 million Euros spent on it, NATO's Computer Incident Response Capability (NCIRC)[845] reached its full organisational and operational capability in May 2014, after a long delay.

5.3.5. The Chicago Summit in 2012

NATO's new cyber defence policy and the Lisbon Summit Declaration were endorsed in the Chicago Summit Declaration:

> *"Cyber-attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which are now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012. We have committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection, to ensure that enhanced cyber defence capabilities protect our collective investment in NATO. We will further integrate cyber defence measures into Alliance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber-attacks. To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase*

[842] There is no information about the fully operational capability of Rapid Reaction Teams now. This full operational capability may be announced by NATO.
[843] NATO (2012), *NATO Rapid Reactions Team to Fight Cyber Attack*, *op.cit*.
[844] *Ibid*.
[845] NCIRC finally has reached its full operational capability in May 2014. "NATO and Cyber Defence" (2013), *op.cit.*

> *concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia.'*'[846]

As already highlighted with the development of cyber technologies, the danger of cyber-attacks has increased, and the structures of cyber terrorist attacks continue to evolve. The Chicago Summit Declaration highlighted the sophistication of potential cyber-attacks. NATO has sought to adapt its strategies in order to address modern day cyber threats as well as other technological threats, humanitarian problems and other terrorist actions. The Chicago Summit reaffirmed that NATO will continue to develop mechanisms designed to prevent cyber-attacks, or, at least, vitiate their effects against itself and its members. However it will remain problematic to decide the next move of cyber terrorists, and the implementation all NATO's policies could prove problematic. These questions were addressed in the Wales Summit of 2014.

5.3.6. The Wales Summit in 2014

The NATO nations met at the Wales Summit 2014. I believe that the Wales Summit is significant because we get a further insight into NATO's concerns regarding cyber threats. For instance, NATO accepted a Defence Planning Package to improve its capabilities against current and future threats. The Declaration states:

> *"NATO needs, now more than ever, modern, robust, and capable forces at high readiness, in the air, on land and at sea, in order to meet current and future challenges. We are committed to further enhancing our capabilities. To this end, today we have agreed a Defence Planning Package with a number of priorities, such as enhancing and reinforcing training and exercises; command and control, including for demanding air operations; intelligence, surveillance, and reconnaissance; NATO's ballistic missile defence capability, in accordance with the decisions taken at the 2010 Lisbon and 2012 Chicago Summits, including the voluntary nature of national contributions; cyber defence; as well as improving the robustness and readiness of our land forces for both collective defence and crisis response. Fulfilment of these priorities will increase the Alliance's collective capabilities and better prepare NATO to address*

[846] NATO (2012), *Chicago Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease (Accessed at: 06/10/2013)

> *current and future threats and challenges. We have agreed this Package in order to inform our defence investments and to improve the capabilities that Allies have in national inventories. In this context, NATO joint air power capabilities require longer-term consideration."*[847]

By adding cyber defence to the overall defence package, The Declaration indicates that NATO continue to view cyber threats as a serious concern that requires collective defence against cyber-attacks. The Summit Declaration went on to endorse an Enhanced Cyber Defence Policy:

> *"As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfilment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."*[848]

The Enhanced Cyber Defence Policy repeated the revised cyber defence policy in terms of prevention and resilience, but the document did not refer to non-duplication, and detection, recovery and defence were later added by NATO nations. The nations again emphasised the main role of NATO as being responsible for defending its own cyber networks, and helping

[847] NATO (2014), *Wales Summit Declaration,* Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (Accessed at: 06/09/2014)
[848] *Ibid.*

or assisting its members if required. The significant point can be noted that this was the first time NATO recognised that international law, international humanitarian law and the UN Charter could apply to cyberspace and cyber threats. Also, the Alliance accepted a threshold of cyber-attacks against its members, which, if reached, the states would invoke Article 5 of the North Atlantic Treaty[849], and the North Atlantic Council would take responsibility for implementation when a case arose under this article. However I would suggest that there is significant omission because the Declaration contains no guidance about where the threshold of cyber-attacks is reached. This raises the obvious question, which cases will trigger Article 5 of the North Atlantic Treaty? The phrase "case by case" suggests that the North Atlantic Council may be reluctant to be part of an aggression against a cyber threat, particularly as NATO has only invoked Article 5 of the North Atlantic Treaty once in its history.

On the other hand, since this decision, there has been a visible improvement regarding the acceptance of cyber threats under international law and Article 5 of the North Atlantic Treaty.[850] Significantly during the Bucharest Summit of 2008, Estonia had called on the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty; however, the cyber-attacks were considered only under Article 4 of the Treaty. Following the endorsement of Enhanced Cyber Defence Policy it can be argued that the NATO will expand their group of experts' remit to evaluate cyber-attacks under Article 4, to include, where necessary an evaluation under Article 5 of the North Atlantic Treaty. The idea was that "*the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under*

[849] Article 5 of the North Atlantic Treaty: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

[850] Chabrow, E. (2014), *NATO Declares Joint Cyber Defence,* Available at: http://www.govinfosecurity.com/nato-declares-joint-cyber-defense-a-7284 (Accessed at: 06/09/2014). "NATO Sets Up Rapid Reaction Force", Available at: http://www.smh.com.au/world/nato-sets-up-rapid-reaction-force-20140905-10d97x.html (Accessed at: 06/09/2014). "NATO to Strengthen Collective Defense", Available at: http://www.aa.com.tr/en/news/384589--nato-to-strengthen-collective-defense (Accessed at: 06/09/2014). "NATO Approves Spearhead Force to Boost Eastern Defences", Available at: http://www.newsweek.com/nato-approves-spearhead-force-boost-eastern-defences-268656 (Accessed at: 06/09/2014). Croft, A. and Holden,M. (2014), *NATO Backs Spearhead Force to Boost Eastern Defenses*, Available at: http://www.chicagotribune.com/news/sns-rt-us-ukraine-crisis-nato-measures-20140905-story.html#page=1 (Accessed at: 06/09/2014). Sarkar, D. (2014), *NATO adopts cybersecurity policy, says such threats, attacks no different from conventional ones,* Available at: http://www.fiercegovernmentit.com/story/nato-adopts-cybersecurity-policy-says-such-threats-attacks-no-different-con/2014-09-05 (Accessed at: 06/09/2014)

Article 5."[851] This suggests that NATO sought to improve its security policy by relying on international law as well as calling for greater cooperation between member states:

> "*We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School and other NATO training and education bodies.*"[852]

NATO has understood the importance of bilateral and multilateral cooperation in providing an effective cyber policy that is capable of stopping or restricting cyber-attacks. Cooperation, bilateral and multilateral agreements and training, exercise and other tools are crucial for effective cyber security policy.

The Wales Summit declaration has an important role in the response to hybrid threats. Before providing details of the declaration, it is crucial to give some details on hybrid threats and hybrid warfare. Hybrid warfare is defined by Lasconjarias and Larsen as: "*these methods exploit non-attributable means like cyber, information warfare, surprise, deception, extensive use of proxy and special forces. On the unconventional side as well, we have also seen the*

[851] Group of Experts Report (2010), *op.cit.*, p.45
[852] NATO (2014), *Wales Summit Declaration, op.cit.*

use of political sabotage, economic pressure, intelligence operations, and special operations. At the same time, we have observed the posturing of conventional forces for a wide range of options for their possible commitment into the conflict. These threats including unconventional and conventional methods referred to as a hybrid war."[853] In short, hybrid warfare can be described as using conventional and unconventional capabilities, including terrorist acts, criminal disorder, cyber threats[854] and economic power to "*achieve synergic effects in the physical and psychological dimensions of conflict in the battle"*.[855] According to Erol and Oğuz, Russia applied hybrid warfare tactics during the Chechnya and Georgia crisis.[856] Russia also used hybrid warfare during the military operations in Crimea and Ukraine.[857] It is clear that a new kind of war has been used by states for their aims.

NATO outlines this threat in the Wales Summit declaration as:

> *"We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces. This will also include enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations, in line with relevant decisions taken, with a view to improving information sharing, political consultations, and staff-to-staff coordination".*[858]

With this explanation, NATO has tried to prepare itself for new kinds of threats in the international arena. Jens Stoltenberg, NATO Secretary General, also gave a speech to the

[853] Breedlove, P. M. (2015), "Foreword", in Lasconjarias, G. and Larsen, J. A. (Eds.) (2015), *NATO's Response to Hybrid Threats*, NDC Forum Paper 24, p. xxii

[854] Reisinger, H. and Golts, A. (2014), "Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence", *Research Paper*, No. 105, p.3; Lasconjarias and Larsen, *op.cit*., p. 4

[855] Renz, B. and Smith, H. (2016), *Russia and Hybrid Warfare: Going Beyond the Label*, Aleksanteri Papers, Available at: http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf (Accessed at: 14/10/2016), pp. 2-3; Hoffman, F. G. (2007), *Conflict in the 21st Century: The Rise of Hybrid War*, Arlington: Potomac Institute for Policy Studies, p. 8

[856] Erol, M. S. and Oğuz, Ş. (2015), "Hybrid Warfare Studies and Russia's Example in Crimea", *Akademik Bakış,* Vol. 9 (17), Available at: http://dergipark.ulakbim.gov.tr/gav/article/viewFile/5000159909/5000144268 (Accessed at: 15/10/2016), p. 267

[857] Popescu, N. (2015), "Hybrid Tactics: Russia and the West", *European Union Institute for Security Studies*, Issue Alert 46, Available at: http://www.iss.europa.eu/uploads/media/Alert_46_Hybrid_Russia.pdf (Accessed at: 14/10/2016), p. 1; Lasconjarias and Larsen, *op.cit*., p. 3. The detail of this hybrid warfare is not given in this research, because these wars are not the scope of the thesis.

[858] *Ibid.*

Press, stating that NATO was going to address hybrid threats and prepare a strategy to fight them.[859]

With the Wales Summit, NATO reviewed its decisions and took new responsibilities against cyber threats. The emphasis on international law and Article 5 of the North Atlantic Treaty were the most influential decisions of the Summit Declaration. The organisation also extended the coverage of cyber threats within the Declaration.

5.3.7. The Warsaw Summit in 2016

During the Warsaw Summit, the Alliance reaffirmed its core tasks as being collective defence, crisis management and cooperative security. Referring to certain security challenges and threats, the document of the Warsaw Summit states:

> *5. There is an arc of insecurity and instability along NATO's periphery and beyond. The Alliance faces a range of security challenges and threats that originate both from the east and from the south; from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks. Russia's aggressive actions, including provocative military activities in the periphery of NATO territory and its demonstrated willingness to attain political goals by the threat and use of force, are a source of regional instability, fundamentally challenge the Alliance, have damaged Euro-Atlantic security, and threaten our long-standing goal of a Europe whole, free, and at peace. Our security is also deeply affected by the security situation in the Middle East and North Africa, which has deteriorated significantly across the whole region. Terrorism, particularly as perpetrated by the so-called Islamic State of Iraq and the Levant (ISIL)/Da'esh, has risen to an unprecedented level of intensity, reaches into all of Allied territory, and now represents an immediate and direct threat to our nations and the international community. Instability in the Middle East and North Africa also contributes to the refugee and migrant crisis.*[860]

NATO strongly warns of the threat of terrorism in the Declaration, and, importantly, that Russia’s current activities increase the unpredictability in the international arena,

[859] NATO (2015), *Press Statements*, Available at: http://www.nato.int/cps/en/natohq/opinions_125361.htm (Accessed at: 14/10/2016)

[860] NATO (2016), *Warsaw Summit Communique*, Available at: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed at: 13/10/2016)

concurrently reducing stability and security.[861] The important point is that although NATO was detailed to explain hybrid threats in the Strategic Concept of 2010[862], the Warsaw Summit Declaration accepts that hybrid threats can be evaluated under Article 5 of the North Atlantic Treaty. According to the Declaration:

> *"We have taken steps to ensure our ability to effectively address the challenges posed by hybrid warfare, where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives. Responding to this challenge, we have adopted a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation. NATO is prepared to assist an Ally at any stage of a hybrid campaign. The Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence. The Council could decide to invoke Article 5 of the Washington Treaty. The Alliance is committed to effective cooperation and coordination with partners and relevant international organisations, in particular the EU, as agreed, in efforts to counter hybrid warfare".*[863]

NATO has accepted the application of Article 5 against cyber threats following the Wales Summit 2014, and with this Declaration, NATO has expanded the coverage of Article 5 against cyber-attacks, including the hybrid contexts. The Declaration also emphasizes the danger of cyber-attacks and current developments on cyber security.[864]

[861] *Ibid*.

[862] Pawlak, P.(2015), "Understanding Hybrid Threats", *European Parliamentary Research Service Blog*, Available at: https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/ (Accessed at: 13/10/2016)

[863] NATO (2016), *op.cit.*

[864] The declaration states that: "70. Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure more effective organisation of NATO's cyber defence and better management of resources, skills, and capabilities. This forms part of NATO's long term adaptation. We continue to implement NATO's Enhanced Policy on Cyber Defence and strengthen NATO's cyber defence capabilities, benefiting from the latest cutting edge technologies. We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable. We will continue to follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace. We

The importance of the Declaration in terms of cyber security is that NATO recognises cyberspace as a domain addition to the existing operational domains of air, sea and land.[865] Secondly, cyber-attacks, including hybrid contexts, can be evaluated under collective defence. Furthermore, NATO encourages its Allies to improve cooperation on cyber defence. It has also improved its partnerships with international organisations and partner nations to adopt effective cyber security policies. The cooperation and exchange of information between states and international organisations is important to the maintenance of good quality cyber security and defence. Now that NATO has proved its capability for improving its security, it gives responsibility to its Alliance to improve their own cyber defences.

5.4. The Application of the Game Theory to NATO's Cyber Defence Policy

There have been many new technological improvements, particularly in cyberspace, and this situation will continue to pose security problems in the future. Since 9/11, the international community recognised the need to take measures to protect themselves from cyber-attacks. However, they are still searching for effective strategies that provide protection from, or vitiate against these types of attacks. NATO been working on cyber security since the Prague Summit of 2002, and is still looking to improve its capability in the area. I will try to explain NATO's cyber security policy in the same way as Estonia's cyber security policy, using the table below, but the different point in the application of Game Theory to NATO's cyber security policy is that two different tables and Game Theory fractions will be used.

Firstly, I would like to use Zero-Sum game to analyse NATO's cyber security policy and then I will use Prisoner's Dilemma.

welcome the work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace.
71. We will ensure that Allies are equipped for, and meet requirements tailored to, the 21st century. Today, through our Cyber Defence Pledge, we have committed to enhance the cyber defences of our national networks and infrastructures, as a matter of priority. Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber-attacks, including in hybrid contexts. Together with the continuous adaptation of NATO's cyber defence capabilities, this will reinforce the Alliance's cyber defence. We are expanding the capabilities and scope of the NATO Cyber Range, where Allies can build skills, enhance expertise, and exchange best practices. We remain committed to close bilateral and multilateral cyber defence cooperation, including on information sharing and situational awareness, education, training, and exercises. Strong partnerships play a key role in effectively addressing cyber challenges. We will continue to deepen cooperation with the EU, as agreed, including through the on-going implementation of the Technical Arrangement that contributes to better prevention and response to cyber-attacks. We will further enhance our partnerships with other international organisations and partner nations, as well as with industry and academia through the NATO Industry Cyber Partnership." NATO (2016), *op.cit.*

[865] NATO (2016), *Cyber Defence*, Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed at: 12/10/2016)

		Cyber-Terrorists	
		Attack	**Do not Attack**
NATO	**High**	**5, -5**	**-2, 2**
	Low	**-2, 2**	**3, -3**

Table 17: Zero-Sum game for NATO’s Cyber Security Policy

The table illustrates expected payoff distribution between NATO and cyber-terrorists. The two sides have two different strategies in the game. NATO will able to choose high level or lower level cyber security policies, and on the other side, cyber-terrorists can choose attack or do not attack. High level security policy can be more expensive than lower level policies, but nevertheless reduces the success rate for cyber-terrorists. The game does not have any pure Nash Equilibrium, and the total of the payoffs are Zero-Sum.

The table can be explained as: NATO did not give much attention to its cyber security until the Estonian cyber-attack, before which the organisation’s cyber security policy was at the lower level. Before 2007, NATO had faced some cyber-attacks, such as during the Kosovo war in 1999. During these attacks, NATO did not have any cyber security policy, and cyber risks and threats were not mentioned in its Strategic Concept. According to the table, cyber-terrorists had payoff of 2 with these attacks, and, on the other side, NATO’s payoff was of -2 and the total was 0.

Since the case of Estonia, NATO has tried to improve its cyber security and has heeded the risk and threats of cyber-attacks in its Strategic Concept. Therefore, the organisation has chosen the play high level security policies. If cyber-terrorists attack during the high level security policies, then the cyber-terrorists will have payoff of -5, because NATO has a strong protection against cyber-attacks. If NATO chooses to play high level security policies, but the cyber-terrorists do not attack, then NATO will have payoff of -2, because the organisation will have given increased attention and resources to cyber security and this may decrease the level of its other security policies. However, in all events, NATO would strongly prefer high level security policies for the protection of the organisation and its members from any attack, and the chosen strategy of cyber-terrorists cannot be known, because this is not under the control of NATO. Therefore, the organisation must choose high level policies to maximize its payoff against cyber-terrorists.

Another application of Game Theory to cyber security is the Prisoner’s Dilemma. Kostyuk applied Prisoner’s Dilemma to the result of the Estonian cyber-attack, and she explained the strategies of Estonia and Russia after the cyber-attacks. I will adapt this application to the cyber security policy of NATO and its relationship with Russia. It is known that NATO established the threat of the former Soviet Union, but, with the collapse of the Soviet Union, NATO changed its shift. Nowadays, Russia is trying to improve its standing in the international arena, which will affect peace and security in international arena. This situation is also mentioned in the Warsaw Declaration. Equally, NATO has tried to improve its cooperation with Russia, and I will evaluate this cooperation under the Prisoner’s Dilemma.

		RUSSIA	
		Cooperate	**Does not Cooperate**
NATO	**Cooperate**	**1)** Individual hackers are punished; **2)** Relationship will increase between NATO and Russia	**1)** Russia does not accept any responsibility; **2)** NATO-Russia relations worsen; **3)** Russia will experience economic losses in accordance with the sanctions by NATO and its members; **4)** Both sides will have more cyber-attacks
	Does not Cooperate	**1)** NATO continues to experience cyber-attacks; **2)** NATO will apply sanctions against Russia; **3)** The Cooperation between NATO and Russia will be decreased	**1)** The cyber-attacks escalate the problem; **2)** NATO can apply to Article 5 of Treaty; **3)** Russia also improves its army against NATO

Table 18: A Prisoners’ Dilemma Game for NATO and Russia[866]

[866] Kostyuk applied Prisoner’s Dilemma to cyber security. Her works is inspirer of the application of Prisoner’s Dilemma to NATO’s policy. Kostyuk applied Prisoner’s Dilemma powerful nation vs. powerful nation and I used this application between NATO and Russia. For more information about the application of Prisoner’s Dilemma to cyber security by Kostyuk; Kostyuk, N. (2013), “The Digital Prisoner’s Dilemma: Challenges and Opportunities for Cooperation”, *World Cyberspace Cooperation Summit IV*, Available at: http://cybersummit.info/sites/cybersummit.info/files/The%20Digital%20Prisoner's%20Dilemma-Challenges%20and%20Opportunities%20for%20Cooperation_Nadiya%20Kostyuk%20.pdf (Accessed at: 12/09/2016)

The international community has faced many cyber-attacks during past decades. Estonia and Georgia have blamed Russia for these attacks, as has Ukraine.[867] Although Russia was blamed for these cyber-attacks, there was no clear evidence.

The table shows the cooperation or non-cooperation between NATO and Russia on cyber-attacks scenarios. The worst scenario for both sides to choose is not to cooperate. According to this scenario, both sides will have more cyber-attacks, which will originate from their territories. Therefore, the crisis will escalate with both sides crossing each other. Also, these attacks may increase the economic loss for both sides, because the trade between NATO members and Russia will decline. Lastly, this scenario might lead to a cyber war. Also, according to Zuesse, if any members of NATO become the victims of the cyber-attacks, then NATO will apply Article 5 of the Treaty for collective defence.[868] This provision includes non-NATO member countries which suffer cyber-attacks originating from other non-NATO members, including Russia. This also increases the tension between NATO and Russia, for if any cyber-attack originates from Russian territory, then we could face the worst scenario.

Other scenarios show the possibilities of the situation in accordance with both sides' strategies. The best scenario for both sides is to choose cooperation, which is a likely scenario, because other options may force them to cooperate with each other. It is known that NATO prefers to try and solve any dispute with peaceful resolutions[869], and would like to cooperate with Russia to improve peace and security in the international arena. Also, the other scenarios would force Russia to cooperate, because if Russia lost its economy, then the country would lose its power in the international arena. Therefore both sides are likely to cooperate.

To sum up, Game Theory can only help NATO, other organisations and states to determine their expected payoffs in the event of possible attacks or no-attacks, and the predictions are important to determine the level of policies. On the other side, the dominant strategy of cyber terrorists can be known through researching the Estonian case. This could help NATO and individual states to improve their cyber security, which would be an advantage for NATO against cyber terrorists. However, the future strategies of cyber terrorists are not known, so predictions in terms of Game Theory are important.

[867] Maza, C. (2016), "Did Ukraine's Cyberattacks Originate in Russia?", *Atlantic Council*, Available at: http://www.atlanticcouncil.org/blogs/new-atlanticist/did-ukraine-s-cyberattacks-originate-in-russia (Accessed at: 15/10/2016)

[868] Zuesse, E. (2016), *NATO Says It Might Now Have Grounds to Attack Russia*, Available at: http://thesaker.is/nato-says-it-might-now-have-grounds-to-attack-russia/ (Accessed at: 12/10/2016)

[869] "What is NATO", Available at: http://www.nato.int/nato-welcome/ (Accessed at: 12/10/2016); Moore, R. R. (2007), *NATO's New Mission: Projecting Stability in a Post-Cold War* World, London: Praeger Security International, p. 58; Borawski, J. and Young, T. D. (2001), *NATO After 2000: The Future of the Euro-Atlantic Alliance*, USA: Praeger Publishers

5.5. The Evaluation of NATO's Policy in the Context of International Law

Details of NATO's cyber security policy were explained in the previous sections, and it is essential to know and criticize the policy under international law and the North Atlantic Treaty. In this part, Articles 4 and 5 of the North Atlantic Treaty will be detailed. Additionally, the researcher will give details of how NATO has applied these Articles of the Treaty, and collective self-defence and collective security will be discussed under a sub-heading. In the second part of the sub-heading, NATO's cyber policy will be evaluated under the UN Charter and the North Atlantic Treaty.

5.5.1. The Application of Articles 4 and 5 of the North Atlantic Treaty

A NATO source mentions the role of NATO as:

> *"The North Atlantic Treaty Organisation was founded in response to the threat posed by the Soviet Union. This is only partially true. In fact, the Alliance's creation was part of a broader effort to serve three purposes: deterring Soviet expansionism, forbidding the revival of nationalist militarism in Europe through a strong North American presence on the continent, and encouraging European political integration."*[870]

Peterson says that NATO was established in 1949, *"to prevent the spread of communist systems further west into the region which became known as West Europe during the Cold War."*[871] In the absence of a Cold War, NATO has extended its mission to protect peace and security:

> *"Since its founding in 1949, the transatlantic Alliance's flexibility, embedded in its original Treaty, has allowed it to suit the different requirements of different times. In the 1950s, the Alliance was a purely defensive organisation. In the 1960s, NATO became a political instrument for détente. In the 1990s, the Alliance was a tool for the stabilization of Eastern Europe and Central Asia through the incorporation of new Partners and Allies. Now NATO has a new mission: extending peace through the strategic projection of security."*[872]

[870] NATO (2014), *A Short History of NATO*, Available at: http://www.nato.int/history/nato-history.html (Accessed at: 04/09/2014)

[871] Peterson, *op.cit*., p. 2

[872] NATO (2014), *op.cit.*

The organisation's role is as security provider to the Allies,[873] and it takes this power from the North Atlantic Treaty. NATO's collective security and defence policies are primarily fixed with Articles 4 and 5 of the North Atlantic Treaty. Article 4 provides that

> *"The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."*[874]

Article 5 states that

> *"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.*
>
> *Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."*[875]

Articles 4 and 5 provide NATO with the power to attack any country which attacks its members or Allies. Additionally, Article 6 of the North Atlantic Treaty supplements Article 5 in terms of endorsing out-of-area actions.[876] According to Article 6 of the Treaty

> *"For the purpose of Article 5, an armed attack on one or more of the Parties is deemed to include an armed attack:*
>
> - *on the territory of any of the Parties in Europe or North America, on the Algerian Departments of France (2), on the territory of or on the Islands under the jurisdiction of any of the Parties in the North Atlantic area north of the Tropic of Cancer;*

[873] Shaw, *op.cit.*, p. 1290

[874] "The North Atlantic Treaty", *op.cit.*

[875] *Ibid.*

[876] NATO (2014), *Collective Defence*, Available at: http://www.nato.int/cps/en/natohq/topics_110496.htm? (Accessed at: 04/09/2014)

> - *on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer."*[877]

The United Nations Charter gives the responsibility of collective self-defence to NATO under Article 51 of the UN Charter. It should be pointed out that Articles 4 and 5 are not the sole legal basis of NATO's actions; Article 7 of the North Atlantic Treaty confirms these articles in terms of legality. According to Article 7 of the North Atlantic Treaty

> *"This Treaty does not affect, and shall not be interpreted as affecting in any way the rights and obligations under the Charter of the Parties which are members of the United Nations, or the primary responsibility of the Security Council for the maintenance of international peace and security."*[878]

Haubler explains Article 7: "*As confirmed by consolidated practice, they are supplemented by Article 7 of the North Atlantic Treaty – which keeps the door open for NATO and NATO-led operations in support of the purposes of the United Nations – and appropriate implied powers of the organisation.*"[879] Obviously these Articles show the connection between the United Nations Charter and the North Atlantic Treaty. It is generally acknowledged that the United Nations Charter is accepted as international law by the international community, and no agreement or organisations shall conflict with the United Nations and its aims. This situation is mentioned in Articles 52/1 of the Charter:

> "*Nothing in the present Charter precludes the existence of regional arrangements or agencies for dealing with such matters relating to the maintenance of international peace and security as are appropriate for regional action provided that such arrangements or agencies and their activities are consistent with the Purposes and Principles of the United Nations.*"[880]

[877] "The North Atlantic Treaty", *op.cit.*
[878] *Ibid.*
[879] Haubler, U. (2010), *Cyber Security and Defence From The Perspective of Articles 4 and 5 of the NATO Treaty,* Available at: http://www.ccdcoe.org/publications/legalproceedings/Haussler_CDfromArticles4and5Perspective.pdf (Accessed at: 10/08/2014), p. 103
[880] "The United Nations Charter", *op.cit.*

Article 51 of the UN Charter gives responsibility for self-defence to NATO if any attacks occur in their areas. It specifies that:

> "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*"[881]

The main point is that of self-defence and other actions, if an armed attack occurs against members of the United Nations. This is mirrored by Article 5 of the North Atlantic Treaty showing a significant overlap between these Articles. Article 2/4 of the United Charter limits the use of force.

> *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*[882]

These Articles complement each other in terms of both peace and security. Kaplan agrees that there is full compatibility of Article 5 of the North Atlantic Treaty with Article 51 of the UN Charter.[883] Also, Haubler cites Beckett's opinion regarding the relationship between Article 5 of the North Atlantic Treaty and Article 51 of the UN Charter as: *"The analysis of Article 5, which 'is the collective self-defence obligation in case of armed attack', likewise reveals similarities. Beckett rightly observes that 'Article 5 of the Treaty uses the same words "armed attack" as occur in Article 51 of the Charter and expressly purports to be based on that Article'. Successfully so, as demonstrated by Beckett's analysis of the statement in Article 5 that 'an armed attack against one or more of the Parties shall be considered to be an attack against them all': this language expresses 'precisely what the inherent right of collective self-defence means'."*[884]

[881] *Ibid.*
[882] *Ibid.*
[883] Kaplan, L. (2007), *NATO 1948: The Birth of the Transatlantic Alliance*, Plymouth: Rowman&Littlefield Publishers, p. 217. Also see, Simma, (1999), *op.cit.*, p.3
[884] Haubler, *op.cit.*, pp. 106-107

NATO's actions, collective defence and security, come under the legal basis of international law. Both the UN Charter and the North Atlantic Treaty explain the use of force against threats in terms of legality, providing that neither the UN nor NATO can use force for aims other than that of collective defence and security.

NATO has invoked Article 5 of the North Atlantic Treaty once since it was established following the terrorist attack on the World Trade Centre in the United States on 11th September, 2001.[885] This was also the first time the UN Security Council and the North Atlantic Council had taken the same decisions on the attacks, under Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty. The harmonisation of these Articles and the cooperation between regional and international organisations occurred in 2001, although this cooperation and broad interpretation of the Articles has not been used since the 9/11 attacks.

Articles 4 and 7 of the North Atlantic Treaty regulate the collective security of the Alliance.[886] Article 4 is used to consult over the concerns of states on matters of territorial integrity, political independence and security. Article 7 of the North Atlantic Treaty outlines the obligations of the members under the UN Charter. Article 2/4 prohibits the use of force, and the Alliance must adhere to this regulation for collective security. If there is a threat to peace and security, NATO cannot directly apply Article 51 of the UN Charter or Article 5 of the North Atlantic Treaty, in such circumstances the UN must also apply Article 39 of the UN Charter which specifies that:

> *"The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41[887] and 42[888], to maintain or restore international peace and security."*[889]

[885] Evans, M. (2003), *International Law*, Oxford: Oxford University Press, p. 605; Also see, Gordon, P. H. (2000), "NATO After 11 September", *The International Institute for Strategic Studies*, Vol. 43 (4), Available at: http://www.brookings.edu/views/articles/gordon/2002wintersurvival.pdf (Accessed at: 10/08/2014), p. 1; Deighton, A. (2002), "The Eleventh of September and Beyond: NATO", *The Political Quarterly*, Vol. 73 (1), Available at: http://onlinelibrary.wiley.com/doi/10.1111/1467-923X.73.s1.9/abstract (Accessed at: 10/08/2014), p. 119; Neuhold, N. (2011), "Legal Crisis Management: Lawfulness and Legitimacy of The Use of Force", in Fastenrath, U., Geiger, R., Kahn, D. E., Paulus, A., Schorlemer, S. V., Vedder, C. (eds.) (2011), *From Bilateralism to Community Interest*, Oxford: Oxford University Press, p.290

[886] Haubler, *op.cit.*, p. 110

[887] Article 41 of the UN Charter: "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and

If the problem continues and threatens peace and security, the UN must apply Articles 40, 41 and 42 to maintain peace and security. If the problem is still not resolved, the UN and NATO can then apply Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty.
For this reason, the UN Charter and the North Atlantic Treaty must be interpreted and applied to maintain peace and security in the international arena. International organisations and NATO cannot directly apply Article 51 of the UN Charter or Article 5 of the North Atlantic Treaty for the use of armed force against an attacker before all legal remedies are exhausted.

5.5.2. A Brief Assessment of NATO's Policy under the International Law[890]

Although the international community has faced some cyber-attacks such as Estonia in 2007 and Georgia in 2008, there was no common approach on what amounts to any cyber-attack can accepted as an armed attack and what the thresholds of Article 5 of the North Atlantic Treaty in terms of collective defence against cyber-attacks.

Furthermore, many questions arise about the use of armed force against cyber-attacks. For instance one critical question is what kind of cyber-attacks should be made in response to the use of force? This question can also be approached from the angle of: when should a cyber-attack face an armed counter-attack? Also, another question that arises is: which legislations should be applied to cyber-attacks? These are the main questions regarding cyber-attacks in terms of international law. Myrli asks the following question about the consequences of cyber-attacks: *"If the source of a cyber-attack can be identified with certainty, which forms of cyber-attack can NATO consider as direct acts of aggression against a Member or Members, and which constitute indirect acts of aggression?"*[891]
The main concern of NATO was how to deal with cyber-attacks, and then to consult Article 4 of the North Atlantic Treaty during the Estonian cyber-attacks.[892] Jens Stoltenberg, NATO Secretary General, states in his speech that "*cyber is now a central part of virtually all crisis and conflicts. NATO has made it clear that cyber-attacks can potentially trigger an Article 5*

of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."

[888] Article 42 of the UN Charter: "Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

[889] "The United Nations Charter", *op.cit.*

[890] The general points of the application of international law to cyber-attacks and cyber terrorism appear in Chapter 4. In this section I will try to explain NATO's policy under international law and therefore this section is not the same as Chapter 4.

[891] NATO Parliamentary Assembly (2009), *op.cit.*

[892] Klimburg, *op.cit.*

response. We need to detect and counter cyber-attacks early; improve our resilience; and be able to recover quickly."[893] It is therefore clear that NATO has accepted the threat and that the organisation will apply Article 5 of the Treaty against cyber-attacks.

The Estonian case is important to the evaluation of this discussion on NATO policy, being not only historically significant, but also in the context of current challenges and international law. The Estonian Government sought the application of Article 5 of the North Atlantic Treaty.[894] Jamie Shea, the head of NATO's Emerging Security Challenges Division said, "*Deterrence is important. We have said for example that Article 5 of NATO's collective defence mechanism could apply in the event of the cyber-attack if that cyber-attack reaches a certain threshold*".[895] However, the Alliance did not consider the application of Article 5[896] to the Estonian cyber-attack, and did not explain the threshold.

At the Bucharest Summit of 2008, the Alliance interpreted cyber threats under Article 4 of the North Atlantic Treaty.[897] The recommendation was that members could consult each other in cases of cyber-attack, but could not assist each other under Article 5 of the North Atlantic Treaty.[898] This illustrates that NATO did not flout the laws where customary international law prohibits the intervention or the use of force.

Returning to 2010 expert report, *NATO 2020: Assured Security; Dynamic Engagement* where it was recognised that, *"the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5.*"[899] The experts[900] agreed the possibility of applying Articles 4 and 5 of the North Atlantic Treaty against cyber-attacks.[901]

[893] "Keynote Speech", Available at: http://www.nato.int/cps/en/natohq/opinions_118435.htm (Accessed at: 13/10/2016)

[894] Rehman, S. (2013), *Estonia's Lessons in Cyberwarfare*, Available at: http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare (Accessed at: 30/08/2014); Poulsen, K. (2007), '*Cyberwar' and Estonia's Panic Attack*, Available at: http://www.wired.com/2007/08/cyber-war-and-e/ (Accessed at: 30/08/2014); Herzog, S. (2011), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses ", *Journal of Strategic Security*, Vol. 4 (2), Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss (Accessed at: 30/08/2014); Traynor, I. (2007), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *The Guardian,* Available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia (Accessed at: 30/08/2014)

[895] "NATO launches 'cyber-attack", Available at: http://www.euronews.com/2013/12/11/nato-launches-cyber-attack-exercises/ (Accessed at: 02/09/2013)

[896] Haubler, *op.cit.* and Tikk, E., *et al., op.cit.*, p. 25

[897] Mcgee, *op.cit.*

[898] "NATO Agrees Common Approach to Cyber Defence" (2012), *op.cit.*

[899] Group of Experts Report (2010), *op.cit.*, p.45

[900] Footnote 454- 37 olacak

[901] Group of Experts Report (2010), *op.cit.*

The decision to apply Article 5 of the North Atlantic Treaty was taken in the Wales Summit in 2014. According to the Declaration,

> *"Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."*[902]

Together with the decision of the Wales Summit in 2014, the cyber defence policy has become part of the collective defence, raising the possibility that the North Atlantic Council will invoke Article 5 of the North Atlantic Treaty against cyber-attacks if one or more members are faced with them. However, the main concern is what a "*case-by-case basis*" means, since it is not explicated in the Declaration, but an important decision was taken in the Warsaw Summit in 2016, when cyber-attacks, including hybrid contexts were accepted for evaluation under the collective defence, Article 5 of the North Atlantic Treaty. I believe that this decision was a milestone in the application of Article 5 of the Treaty on cyber-attacks, because I think NATO defined one of the thresholds of cyber-attacks with this Declaration.

All in all, it is important to encourage member states to define the use of force under Articles 4 and 5 of the North Article Treaty. The actions and decisions of NATO show us that the organisation will apply Article 5 of the North Atlantic Treaty to cyber-attacks. As mentioned above, NATO is a peaceful organisation and tries to resolve conflicts with peaceful solutions. Therefore when a cyber-attack requires the application of Article 5 of the Treaty, if the conflict cannot be solved with peaceful solutions, then NATO can invoke its members to apply Article 5 of the Treaty.

5.6. Assessment and Recommendations

5.6.1. Assessment

NATO's cyber security policy has been mentioned in detail above and in this section the policy will be examined and the cyber policy of NATO will be critiqued. Every policy has negative and positive consequences. NATO has been improving its cyber security policy since the Prague Summit of 2002, and from this point, the organisation has prepared

[902] NATO (2014), *Wales Summit Declaration, op.cit.*

documents, had meetings and conducted plans to obstruct cyber threats. The cyber security policy was outlined for the first time in the Strategic Concept of 2010. This means that NATO has been more concerned with cyber threats than previously, and many comprehensive meetings, documents and plans have been prepared. However, although NATO has taken some measures and creates institutions to prevent cyber-attacks, NATO sometimes did not finish these institutions in the expected time. For instance, the NCIRC normally had full operational capability by the end of 2012, but it reached reach its full capacity in May 2014. As mentioned above, the policies may be accepted, but the implementation process is too slow, which will be a problem in future in terms of protecting security. The delays in reaching full capabilities of organisations are too long, and therefore NATO must resolve this.

Returning to the support and encouragement of members by NATO, NATO encourages regional and international cooperation as a key deterrent against global cyber threats. Although NATO does encourage its members to sign and implement international agreements, the members may be reluctant or apply these conventions or agreements very late in this regard. The common cybercrime agreement is the Convention on Cybercrime agreed by the Council of Europe, but Turkey has signed this, in 2010, and ratified it in the second part of 2014. This shows us that the implementation process takes too much time.

Although NATO has taken steps to stop cyber-attacks, there have been many cyber-attacks against the organisation,[903] some of which have not been made public. An offensive policy may affect NATO in terms of its defence policy against terrorists. For instance, if the main aim of their cyber defence policy is resilience, if terrorists attack the defences of NATO, the policy will not work and the terrorists would gain advantage against NATO and its members. Whilst NATO and its staff may improve their ability and capability on the one hand, but on the other, terrorists can improve their abilities too, because they do not have restrictions, such as legality. NATO's policies must be based on a legal framework, but terrorists do not use moral values or legality. As mentioned above, offensive strategies will have more outcomes against the defensive policies. Also, the cost of the policies will be more extortionate than its attackers' policies, because terrorists do not need finances for their attacks; they only need a computer, and the ability to attack any vulnerability. However, NATO, on the other hand, must pay money to improve the capacity of the 58 million Euros NCIRC, whilst not having a specific income. The balance of NATO may change from period to period, and there is no

[903] For more details; "The History of Cyber Attacks: A Timeline", *NATO Review*, Available at: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (Accessed at: 11/11/2013)

regular payment to the organisation from its members, which is another problem for NATO. If there is no money, NATO cannot fix its policy.

Lastly, the evaluation of cyber-attacks under Article 5 of the Treaty is important for the Allies, because with this declaration, cyber-terrorists, or their financiers and supporters will think twice before attacking NATO or its Allies. Also, the scope of cyber-attacks has been extended to acknowledge hybrid threats and evaluate them under Article 5. These are the positive aspects of the cyber security policy of NATO.

The next section offers some recommendations to achieve the most effective cyber security policy.

5.6.2. Recommendations

Following the specification of the negative consequences of NATO's cyber policy, some recommendations should be offered.

The policy of NATO does not have totally negative consequences. NATO has had some success in implementing and applying new policies on cyber threats. For example, the CCDCOE have produced new ideas to fight against cyber threats, establishing new institutions and creating a Rapid Reaction Team to help member states if required. These are some of the successful points of NATO. However I will offer some recommendations to suggest new solutions to fight against cyber threats.

The first recommendation is to once again simply call for a common definition of cyber-terrorism. Although it can be said that cyber threat is a new element in the concept of terrorism, despite its wide historical background, it does not have a cohesive definition. Every state has its own definition, which causes a dilemma between states in terms of identifying any situation or threat. Additionally, states have different policies and ways to stop these threats. The lack of a common understanding creates uncertainty, so it is important to decide on a shared definition in order to address the indeterminate situations that may arise between states and the international community. If the international community had a common definition on problematic concepts such as terrorism and cyber terrorism, the first stage of the problem could be solved, and regional and international organisations could work together efficiently to stop these kinds of threats. The first step to be taken by the international community is to define the concept. As mentioned in previous chapters, the concept of cyber terrorism can be defined as: "*a motivated attack by terrorists, attackers, or sub-national groups against target states using cyber space in order to harm and destroy national and international critical infrastructure, including communication, transportation, energy,* *security, SCADA and banking systems, as well as personal information, and the threatening of people in the states and international arena for the purpose of achieving political, cultural, or economic aims*." The benefit of this definition is that it covers all areas, such as political, economic and social objectives, and includes the intention to harm and destroy. The definitions given in Chapter 1 did not cover all of these objectives, and scholars have evaluated them separately. I believe that the common definition outlined above could solve the international community's common understanding difficulty, allowing them to focus on the problem directly.

The second recommendation is that the international community must decide on how and when to implement and apply international laws to fight against threats such as cyber terrorism. There are many arguments about the application of the UN Charter and North Atlantic Treaty against cyber-attacks. The international community must draw up and decide on international legal measures. For example, if the UN Security Council has no clear resolutions, any action may be seen as illegal, and sometimes the UN Security Council has different resolutions and decisions on the same argument. If the UN and NATO want to survive, these organisations must be equal, and decide on solutions within the international law, not according to their individual interests. I do not believe that it is possible to solve this problem without the support of the UN Security Council members. This will be a dream, but if more states become part of the UN Security Council and the five permanent members do not have any veto power,[904] the UN could be equal and powerful in the international arena.

My third recommendation would be to redraft national law so it has some synchronicity with international law. For instance, as mentioned above, the common cybercrime agreement was the Convention on Cybercrime, agreed by the Council of Europe, but Turkey signed and ratified it in 2014, as a member of NATO. However Turkey has not implemented these conventions into its own national laws. NATO must encourage and support its members to sign and ratify international agreements and to implement these legislations into their national laws. This will help to equalise the legal systems of the members of NATO, and the differences arising from the legal systems of individual states will be resolved.

The fourth recommendation of an effective policy is that each state must have cyber experts and manage new experts who know the game plan. Cyber terrorists will aim to use cyberspace more effectively than the state experts, so the latter must know the cyber terrorists'

[904] If one of the permanent members of the UN rejects any resolution, the Security Council cannot make any decision on any problems. This is called a veto power. This problem was experienced during the Cold War and after 1991. However, the Security Council members and permanent members can use this power even if they do not have any interest in a case.

game/attack plan in order to fight against them. If the state experts know the next step of the game, the cyber terrorists will lose and not have any more effect than anticipated. Additionally, the members of NATO should support CCDCOE's initiatives and send their experts to the CCDCOE to learn about new policies. Training and exchange of plans or policies will help to improve the cyber security policies of the individual states.

The fifth recommendation of an effective cyber policy is that new bilateral and multilateral agreements should be signed by states. In this way, they can share their experiences. It may be difficult to find cyber attackers because cyberspace is so vast, and terrorists and attackers can take advantages of cyberspace for their aims. Therefore, bilateral and multilateral agreements between states associated with international agreements can be crucial and critical to resolve the problems which stems from cyberspace. Furthermore, NATO will have bilateral and multilateral agreements with other regional and international organisations, such as the European Union, the Telecommunication Union and the UN.

Furthermore, the UN and NATO must work together to counter cyber-attacks. These two organisations are vital for the international community, since their decisions will affect the world and their institutions will use international law to help states fight against cyber-attacks. Moreover, NATO should seek to improve its relationship with non-member states, such as Russia, China, Japan, India and Brazil. By improving its relationship with these states, NATO's cyber plan could include these states and the exchange of cyber security plans. In accordance with the exchange of information, NATO and its members would learn and know more about other cyber policies and alternative plans.

Moreover, NATO and its member states should try to locate their own open doors against cyber-attacks via related exercises. Cyber exercises must be conducted by the CCDCOE, and NATO should encourage its members to participate. Also, these types of exercises could be done with other non-member states, and regional and international organisations.

The last recommendation is necessary to ensure effective cyber security, because, while the other recommendations were directed at NATO member states in particular to improve their abilities against cyber threats, this recommendation also covers all states. The ICC jurisdiction should cover terrorism and cyber-terrorism. As mentioned in Chapter 2, the jurisdiction of the ICC on the crime of terrorism was rejected by states, because they did not have any agreement on a common definition of the concept. We are again coming back to first recommendation, which is the lack of a common definition of the concepts. When this problem has been solved, then these crimes can be added to the jurisdiction of the ICC. The policies will be supported by international law and international jurisdiction with the acceptance of the crime of terrorism and cyber terrorism under the Statute of the ICC.

Some recommendations have been made by the researcher, and if the international community had a strong cyber security policy, it would comply with these recommendations and others determined by states and organisations. If one of them is missed, the international community can forget about effective cyber security. Cyber terrorism and cyber threats are different from other threats. For example, it is almost impossible to find the criminals. Cyber terrorism can be conducted from anywhere in the world and uses the advantage of cyberspace, so the international community should work together to stop cyber threats.

5.7. Conclusion

As explained above, NATO has tried to improve its capability against cyber-attacks. The main aim was to portray NATO's policy in detail since the first attack emerged in 1999, and to evaluate this policy under the Game Theory. The other aims were to draw attention to the important points of cyber threats and criticize the policy of NATO.

Although it has some advantages, NATO has not found an effective policy to fight against cyber threats. This is because NATO members do not have the same level of technological improvements or the same policies, and some members, such as Turkey has still tried to fix its cyber security policy. On the other hand, although some NATO members do not have adequate policies themselves to fight against cyber threats or attacks, NATO has still evolved its policy conceptually and practically. One of the main issues is that NATO has tried to protect its own cyber infrastructure, and if Allies need help and request it, NATO will help. This shows that NATO must try to fix its own cyber systems. In my opinion, without equal cyber policies between NATO members, it will be unable to protect its own cyber systems.

From the Prague Summit in 2002 to the Wales Summit in 2014, there has been a visible improvement in the cyber security policy of NATO. The organisation has started to establish institutions for creating cyber security policies, and now the policies are clearer and supported by international law, although the application of the laws is not clear.

The main role of the Rapid Reaction Team is to help and assist states under attack, and when the team comes on board to help any state, the experts will learn more about the kind of cyber-attack, and offer new ways for states and NATO to prevent similar attacks. In addition, NATO has to pay more money to the Rapid Reaction Teams to improve their own capabilities, and this situation will create financial burdens on NATO. If we again apply our simple evaluation using Game Theory, we could say that when NATO creates and improves the Rapid Reaction Team, it must pay more money; however, if NATO does not do this, the cyber attackers' actions could be more effective than before. More money and more powerful institutions ensure less effective cyber-attacks, whereas less money and weaker institutions will lead to more effective cyber-attacks. Therefore, in the Game, the weaker side will lose everything and the other side will win more payoffs. This situation will create the Zero Sum Game fraction for both sides.

If NATO does not come to an international agreement on the definition of cyber threats and decide which threats can be evaluated under which laws, it will not be possible to determine its effectiveness. An effective policy would be accepted as establishing harmony between the policy and legislations. As mentioned in previous sections, international laws and policies have a mutual relationship. If there is no cooperation between them, actions and policies will be illegal, and international laws will lose their importance.

Although NATO has improved its cyber security and tries to help its members if requested, the organisation has a long way to go to counter cyber threats. NATO member states must support and implement NATO's cyber security policy rules as part of NATO. If the members do not support the policies as one body, NATO will lose its significance. The final point of the chapter is that NATO must accept recommendations on how to fight against cyber threats, warn its members about the use of cyber-attacks against states and the international community, and be strict in the application of international laws.

CHAPTER 6: THE CYBER SECURITY POLICY OF TURKEY

6.1. Introduction

Turkey's defence policy, just like that of other developing countries,[905] is still evolving and improving in terms of their adopting new policies which would harmonize their nation's law with that of international and bilateral agreements, as well as establishing new institutions for the purpose of fighting against cyber threats. Turkey had already evaluated cyber threats, including cyber terrorism and cyber espionage, as being "cybercrime". The first cybercrime law which were passed in order to combat cyber threats were accepted in 1991.[906] Since that time, Turkey has accepted, added, rearranged and adapted some of its laws in order to fight against modern cyber threats. These legislations will be detailed in the next sections of the chapter for the purpose of understanding why Turkey has accepted and implemented these legislations. The problem of cyber threats, however, has also evolved and has affected some important institutions in Turkey, since, even though some ministry websites and information infrastructures were able to block these attacks, others were not so lucky and many documents were stolen in the attacks on the Board of Higher Education in 2012.[907] Following these attacks, Turkey has shown its awareness of such threats, and has resolved to tackle the issue by implementing national law and adopting cyber security policies. More details about this national law against cyber threats, and the cyber security policy will be detailed in this chapter.

With its awareness of those threats, Turkey adopted an Action Plan in 2013 to improve its cyber security for the purpose of better coping against any cyber-attacks. This Action Plan signifies the first time that Turkey has tried to take more responsibility to stop these kinds of attacks. Also, in accordance with the NATO decision of 2011, the Turkish Armed Forces

[905] "Developing Countries", Available at: http://www.isi-web.org/component/content/article/5-root/root/81-developing (Accessed at: 01/02/2014)

[906] 3756 nolu Kanun (1991), *765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun*, Sayı: 20901, Available at: http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf (Accessed at: 10/11/2013)

[907] "Ve Türkiye'ye Siber Saldırı Başladı", Available at: http://www.posta.com.tr/guncel/HaberDetay/Ve_Turkiye_ye_siber_saldiri_basladi.htm?ArticleID=75372%20%20%20%20%20%20%20%20%20%20%20&Date=19.04.2010&PageIndex=2 (Accessed at: 10/09/2014). "Türkiye'ye Siber Saldırı Tehdidi", Available at: http://www.dunya.com/turkiyeye-siber-saldiri-tehdidi-152944h.htm (Accessed at: 10/09/2014). "YÖK'e Siber Saldırı", Available at: http://www.gazetevatan.com/yok-e-siber-saldiri--503255-gundem/ (Accessed at: 10/09/2014). "Hackerler YÖK'e 123456 Şifresiyle Girmiş", Available at: http://www.memurlar.net/haber/327857/2.sayfa (Accessed at: 10/09/2014)

established an institution in 2012[908] called the General Staff Warfare and Cyber Defence Command.[909]

It must be mentioned here that there have been many problems and benefits in studying this topic. For instance, the following problems were experienced whilst writing about the research topic: there is little information regarding the cyber policy of Turkey, and it is not possible to discover any further details about these policies primarily due to there being security problems in Turkey preventing information being obtained from state officials. Therefore, this research will have some limitations in light of these problems. I have tried to contact some experts and officials in order to gain more information about the country's cyber policy.

Largely due to these limitations, Turkish academics and commentators have based their research on cyber- crime on outdated material, impeding improvement and hindering the production of original works. I seek to 'close the academic gap' in Turkey by providing more detailed information about the cyber security policy of Turkey, including assessment and recommendations. In addition, it is hoped that this chapter and research will show and encourage academics to work on different topics in Turkey.

Books, articles and internet resources will be utilised for the purpose of explaining, understanding and criticising the cyber security policies of Turkey.

In this chapter, the country's cyber security policy will be analysed and criticised in some detail. The chapter is divided into four different parts. In the first section, Turkey's cyber defence policy will be evaluated and criticized. Furthermore, the cyber exercises, which were TR-BOME Cyber Exercise 2008**,** National Cyber Security Exercise 2011, Cyber Shield Exercise 2012 and National Cyber Security Exercise 2013, and other key processes, will also be detailed in this section, for the purpose of better understanding how Turkey has improved its cyber security policies. It is valuable to know how Turkey started to make improvements on its cyber capabilities and cyber exercises, in order to identify the problems that the country has faced with relation to building a better cyber infrastructure. Findings from the early cyber

[908] See Chapter 5 for more details

[909] Gramaglia, M., Tuohy, E. and Pernik, P (2013), "Military Cyber Defence Structures of NATO Members: An Overview", *Background Paper*, Available at: http://icds.ee/fileadmin/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf (Accessed at: 08/09/2014). "Turkish Army's New Cyber Defence Unit", Available at: http://www.aa.com.tr/en/news/124195--turkish-armys-new-cyber-defense-unit (Accessed at: 08/09/2014). "International Cyber and Security Conference Was Held in Ankara", Available at: http://www.defence-turkey.com/?p=article&i=1405 (Accessed at: 08/09/2014)

exercises will be provided, in order to glean insight into why Turkey did not care about its cyber security until the 2000s.

In the second section of this chapter, cybercrime will be reviewed in terms of Turkish national law, and more details will be given here about the national law applicable to cybercrime and cyber threats. Also, where Turkey has signed, ratified, or is a part of any international, bilateral or multilateral agreements, these will also be mentioned in this part of the chapter. The point of this section is to explain national and international laws which Turkey is a part of concerning cyber threats. Furthermore, the brief historical background of Turkey's national law against cyber threats will also be criticized in this section.

In the third section of this chapter, I will try to evaluate Turkey's cyber policy with the help of Game Theory. Some important interpretations will be gained from this theory which will explain Turkey's strategic situation with regards to its cyber security, but a full analysis will only be provided in the last section. I believe that Game Theory could help Turkey to improve its cyber capabilities in terms of identifying its weaknesses contra cyber terrorists, and provide it with the tools needed for producing new strategies in order to fight against cyber-attacks.

Finally, in the last section of this chapter, Turkey's cyber policy will be assessed. The researcher will recommend that Turkey should strengthen its cyber capabilities, and therefore, the researcher will offer some recommendations in order to help with this improvement. Of course, some critical developments have been made in Turkey, but Turkey needs more than that. Thus, I will also attempt to offer different ideas about improving Turkey's cyber security capabilities.

6.2. The Evaluation of the Turkish Cyber Defence Policy

Turkey did not show any apparent concerns about its own cyber defence policy until hackers and attackers started to threatened the security of the country. Although Turkey had some law concerning cybercrime in its national law from 1991, it did not have any policies regarding cyber security. Furthermore, this did not change until the mid-2000s, because little consideration was given to the effects of cyber threats. It is also perhaps worth noting that Turkey did not have full internet connection until the mid-2000s. An evaluation of cyber threats under Turkish national law will not be given in this section. Rather, the main aim is to discuss and evaluate how Turkey has tried to improve its cyber security.

Although Turkey's first cyber security policy in terms of National Law, Law number 3756, was accepted in 1991,[910] the Turkish Parliament did not concurrently adopt a policy which would have fought against cyber threats. The Turkish Parliament and Turkish officials tried to solve these problems simply by utilising legal devices, such as adapting provisions of law to the National Law but it wasn't until the mid-2000s that Turkey began to adopt official policies for fighting against cyber terrorism and threats.

The Information Society Strategy Action Plan 2006-2010 which was drafted by the State Planning Organisation. According to paragraph 87 of the document, "*regulations will be enacted and implemented with regard to the legal infrastructure in line with the purpose of ensuring the protection of information concerning national security on the electronic environment, and development of the country's information security systems. Secondly, The Bill on Protection of Personal Data Privacy will be enacted*."[911] Together with this Action Plan, Turkish officials sought to protect security-sensitive information by legislations. In addition, paragraph 88 of the document provided that:

> *"A 'computer emergency response team' (CERT) will be established, to constantly track security threats in cyberspace, publish warnings, provide information on precautions that can be taken against these risks, and coordinate counter-measures in case of realized risks. Minimum security levels required for public institutions will be defined based on agencies and transactions; the security levels of the systems, the software and the networks used by agencies will be identified and recommendations will be proposed to fix any shortcomings.*"[912]

Thus, by accepting paragraph 88 of the Information Society Strategy Action Plan 2006-2010, TR-BOME[913] (CERT) was established and coordinated by The Scientific and Technological Research Council of Turkey National Research Institute of Electronics and Cryptology (TUBITAK UEKAE).[914]

[910] 3756 nolu Kanun (1991), *op.cit.*

[911] State Planning Organisation (2006), *Information Society Strategy Action Plan 2006-2010,* Available at: http://www.bilgitoplumu.gov.tr/Documents/5/Documents/060700_ActionPlan.pdf (Accessed at: 11/09/2014), p. 38

[912] *Ibid*.

[913] The expanded Turkish of this acronym is as follows: Bilgisayar Olaylarına Müdahale Ekibi

[914] Bahşi, H. and Karabacak, B. (2008), *Ulusal Bilgi Sistemleri Güvenlik Programı,* Available at: http://www.emo.org.tr/ekler/d823125670f66de_ek.pdf (Accessed at: 11/09/2014), p.146. Ünver, M., Canbay, C. and Mirzaoğlu, A. G. (2011), *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*, Available at: http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/dokumanlar/sibergstmct.pdf (Accessed at: 12/09/2014), p.37. Türkiye Büyük Millet Meclisi (2012), *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal*

The main duty of the TR-BOME (CERT) is "*to help institutions and organisations throughout the country in gaining the ability to deal with computer security incidents; and to respond to computer security incidents when they happen*."[915] Turkish officials saw cyber threats as an important security problem, and tried to fix the systems by creating these institutions.

The more information will be given about why Turkish officials gave this responsibility to TUBITAK. TUBITAK's role is explained in its website as:

> "*The Scientific and Technological Research Council of Turkey (TÜBİTAK) is the leading agency for management, funding and conduct of research in Turkey. It was established in 1963 with a mission to advance science and technology, conduct research and support Turkish researchers. The Council is an autonomous institution and is governed by a Scientific Board whose members this selected from prominent scholars from universities, industry and research institutions.*"[916]

TUBITAK created an Information Centre in 1996 called "*The Turkish Academic Network and Information Centre (ULAKBIM)*". The main objectives and aims of the Centre is that of:

> *"... operating a high speed computer network enabling interaction within the institutional elements of the national innovation system, and providing information technology support and information services to help scientific production. ULAKBIM aims at providing technological facilities such as computer networks, information technology support, and information and document delivery services, to meet the information requirements of universities and research institutions, and to increase the efficiency and productivity of their end users. ULAKBIM consists of National Academic Network (ULAKNET) Unit, which undertakes the task of formation and operation of research and education network infrastructure in Turkey, and Cahit Arf Information Centre, which provides information and document supply services nationwide".*[917]

Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu, Available at: http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf (Accessed at: 12/09/2014), p.774

[915] "About TR-CERT", Available at: http://www.bilgiguvenligi.gov.tr/about-tr-cert.html (Accessed at: 12/09/2014)

[916] "Who We Are", Available at: http://www.tubitak.gov.tr/en/about-us/content-who-we-are (Accessed at: 12/09/2014)

[917] "Turkish Academic Network and Information Centre", Available at: http://www.ulakbim.gov.tr/eng / (Accessed at: 13/09/2014)

Together with the creation of ULAKBIM, the organisation has established ULAKNET (Network Technologies Department),[918] and this institution provides coordination between universities and research centres. With the emergence of the need for cyber security, TUBITAK has tried to improve public awareness about cyber security. This is why ULAK-CSIRT (Computer Security Incident Response Team) was established in 2006 by TUBITAK.[919] The main aim of ULAK-CSIRT is that of "*preventing the potential security violation of external networks to ULAKNET, ascertaining the* [nature of] *attacks and the people in charge and in the same way, preventing the attacks of ULAKNET to the outside world and if there was an attack, ascertaining the people in charge of the attack and sharing the information with the administrators of this network.*"[920]

Additional objectives of ULAK-CSIRT are mentioned as:

- *Increasing the consciousness of information security throughout the network,*
- *Decreasing the number of the attacks threatening the computer security of the academic network,*
- *Coordinating the stage of ascending the people in charge of security violation,*
- *Informing the administrators of nodes who are connected to the network about the up-to-date deficits and their solutions,*
- *Training the connected node administrators about information security,*
- *Supplying documents in Turkish about the methods of providing information security.*[921]

It can be accepted that TUBITAK has more experience with cyber security than any other Turkish organisation or institution; therefore, this institution's responsibility may improve Turkey's cyber infrastructure and security capabilities.

[918] "About ULAKNET (Network Technologies Department)", Available at: http://www.ulakbim.gov.tr/eng/ulaknet/ (Accessed at: 13/09/2014)

[919] Soysal, M., Karaarslan, E., Eryol, G., and Yüce, H. (2006), "Ulaknet Bilgisayar Olaylarına Müdahale Birimi ULAK-CSIRT Deneyimi", XI. "*Türkiye'de İnternet" Konferansı Bildirileri*, Available at: http://inet-tr.org.tr/inetconf11/kitap/soysal_karaarslan_inet06.pdf (Accessed at: 13/09/2014), p.84

[920] "ULAK-CSIRT", Available at: http://csirt.ulakbim.gov.tr/eng/ (Accessed at: 13/09/2014)

[921] *Ibid.*

6.2.1. TR-BOME Cyber Exercise 2008

After the creation of the TR-BOME (CERT), Turkey conducted its first cyber exercise in 2008. This cyber exercise was coordinated by TR-BOME.[922] The aim of the exercise was for the purpose of controlling the cooperation processes of the TR-BOME. Only eight organisations and institutions participated in this cyber exercise.[923] During the exercise, some problems were found, and mentioned in the report. [924] For instance, the participating corporations could not send any signed emails from their systems; moreover, some of their systems were not able to recognize those emails, or prevent them.[925] In addition, the report offered some recommendations to these institutions for resolving their problems, such as: The email addresses which was using for information, should be updated annually; Security records systems should be analysed in different periods; The institutions should cooperate with TR-BOME; The cooperation and information should be improved and training should be provided to these staff.[926]

This cyber exercise had advantages and disadvantages in terms of improving the cyber capabilities of Turkey. Its advantage was that of showing up Turkish institutions' weaknesses; hence that they should improve their capabilities. On the other hand, with only eight institutions participating in this exercise, many of the key Turkish institutions either did not participate, or were not invited to take part in the exercise. The Turkish Ministries of Defence, Finance, Transport, and the Interior, as well as the Turkish Armed Forces, the National Intelligence Organisation, and the Turkish National Police should participate in such cyber exercises in order to ascertain their weaknesses, and fight against any potential cyber-attacks, but these organisations and institutions were not invited to take part, and there was no clear explanation for this. As is known, the terrorists' main aim is that of awakening fear amongst a great number of societies; therefore, they are most likely to attack important national

[922] Ünal, T. (2008), "BOME 2008 Bilgi Sistemleri Güvenliği Tatbikatı: Tatbikat Sonuç Raporu, *Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü*, Available at: https://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/bilgi-sistemleri-guvenligi-tatbikati-bome-2008.html (Accessed at: 15/09/2014). Bakır, E. (2012), "Türkiye'de Siber Güvenlik", *Bilim ve Teknik*, Kasım, Available at: http://vizyon21yy.com/documan/genel_konular/bilisim/Turkiyede_Siber_Guvenlik.pdf (Accessed at: 15/09/2014), p. 14. İstanbul Ticaret Odası (2011), "Bilişim Teknolojileri ve e-Ticaret Şubesi", *Bilişim ve e-Ticaret Bülteni*, Şubat, Available at: http://www.ito.org.tr/itoyayin/SY059208.pdf (Accessed at: 15/09/2014), pp.7-8

[923] These institutions were: the Presidency of the Republic of Turkey, the Turkish Prime Ministry, the Turkish Ministry of Justice, the Turkish Courts of Accounts, the Turkish Under-Secretariat of the Treasury, the Central Bank of the Republic of Turkey, the Capital Markets Board of Turkey, and the General Directorate of Land Registry and Cadastre.

[924] Ünal, *op.cit.*

[925] *Ibid.*

[926] *Ibid.*

institutions in order to accomplish their aims. I believe that this is one of the disadvantages of this particular cyber exercise. Another disadvantage of the cyber exercise is that it took place in a narrow area, only covering those institutions with which the TR-BOME cooperated. Nevertheless, it is important to examine the other side in terrorist attacks, by thinking like them. Therefore, I believe that, although Turkey was trying to improve its cyber security capabilities with this exercise, it only demonstrated the incompetence of the employees of the IT departments.

6.2.2. Working Group Report

Together with Turkey's development of cyber security policies, a working group was established under the coordination of the TUBITAK UEKAE[927] in 2008.[928] Many public organisations and institutions participated in this working group.[929] The working group report, which was published in 2009, mentioned some risks with regards to communications and information systems. Turhan lists these risks[930] as follows:

- *Many of the public organisations and private institutions provide their services over the Internet;*
- *Critical information and the infrastructure of the communication systems are connected to the Internet;*

[927] TUBITAK explains the role of UEKAE as follows: The "*UEKAE puts signatures to dozens of projects in the fields of cryptology and advanced electronics, [and] produces solutions for [the] military and civil needs of our country. The National Research Institute of Electronics and Cryptology is an R&D organisation that develops information security and electronic system projects vital to strategic government institutions, making significant contributions to Turkey's ability in information security.*" "National Research Institute of Electronics and Cryptology", Available at: http://uekae.bilgem.tubitak.gov.tr/en/kurumsal/national-research-institute-electronics-and-cryptology (Accessed at: 15/09/2014)

[928] Karabacak, B. (2010), *İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları*, Available at: https://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html (Accessed at: 16/09/2014). Ünver *et al., op.cit.* p. 25. Türkiye Büyük Millet Meclisi (2012), "Bilgi Güvenliği ve Bilişim Suçları", *Biak Raporu*, Available at: http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf (Accessed at: 16/09/2014), pp. 776-778

[929] These institutions include: the Presidency of the Republic of Turkey, the Prime Ministry, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Defence, the Ministry of Finance, the Ministry of Transport, the Ministry of the Interior, the Turkish Armed Forces, the State Planning Organisation, the Under-Secretariat of the Treasury, the Central Bank of the Republic of Turkey, the Republic of Turkey's Secretariat-General of the National Security Council, the National Intelligence Organisation, the Turkish National Police, the Banking Regulation and Supervision Agency, the Information and Communications Technologies Authority, and TUBITAK UEKAE.

[930] I have tried to locate the original report to add my work, but I could not find the document and my sources did not give me any information about the document. This is why I have had to revert to Meltem Turhan's information regarding the report.

- *The usual update of the communication and information systems, preparation of the technological projects for the [purpose of] using communication and information systems in the critical services;*
- *The influence of information technologies on the public;*
- *The problem of accepting the security of the communication and information systems only by Computing institutions;*
- *There being less information about organisations utilising communication and information technologies, and there not being a leading feature;*
- *The presence of foreign dependence on hardware and software;*
- *Insufficient information on the information processing units of public employees;*
- *There are not being a sufficient level of awareness about the corporation and its personal;*
- *The insufficient structuring of the public units;*
- *No one considering security being an important element of communication and information systems.*[931]

In accordance with the risks of communication and information systems, some solutions were offered in the report. These solutions were mentioned in Turhan's paper and in the BIAK Reports, and include:

- *The creation of legal regulations;*
- *Improving the country's cyber capabilities;*
- *The establishment of the National Computer Incident Response Organisation;*
- *Collecting information and raising awareness about cyber threats;*
- *Ensuring the security of the National Critical Infrastructure Information System;*
- *Ensuring international coordination;*
- *Ensuring the security of corporate information and communication systems;*

[931] Turhan, M. (2010), "Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri", *Uzmanlık Tezi Bilgi Teknolojileri ve İletişim Kurumu*, p. 121

- *Preparing the National Virtual Environment Security Strategy*.[932]

Even though the BIAK Report was prepared and some solutions were accepted, according to Unver *et al.*, it does not recommend any steps for applying these strategies.[933]

As may clearly be discerned, according to the above report, some risks were found and some solutions were accepted. However, the implementation of these strategies, plans and policies proved difficult in Turkey, primarily because of state bureaucracy and the lack of qualified and knowledgeable personnel in top positions.

6.2.3. The Meeting of the National Security Council

Along with the creation of the TR-BOME and acceptance of the working group's report, another security policy was adopted by Turkey during the last part of 2010. The National Security Council met on 27th October, 2010 to discuss security problems. It is prudent, however, to first explain what the National Security Council is at this point. Article 118 of the Constitution of the Republic of Turkey explains that the duty of the National Security Council is that of

> *"... submit[ing] to the Council of Ministers its views on the advisory decisions that are taken and ensuring the necessary condition with regard to the formulation, establishment, and implementation of the national security policy of the state. The Council of Ministers shall evaluate decisions of the National Security Council concerning the measures that it deems necessary for the preservation of the existence and independence of the state, the integrity and indivisibility of the country and the peace and security of society."*[934]

The National Security Council [935] therefore has the responsibility of offering its recommendations regarding the country's national security.

[932] Türkiye Büyük Millet Meclisi, p. 778. Turhan, *op. cit.*,p.122

[933] Ünver *et.al., op.cit.*, p. 26

[934] "The Constitution of the Republic of Turkey", Available at: http://www.hri.org/docs/turkey/part_iii_2.html (Accessed at: 15/09/2014)

[935] The National Security Council members are: President, Prime Minister, Commander of the Turkish Armed Forces, Deputy Prime Ministers, Minister of Justice, Minister of National Defence, Minister of the Interior, Minister of Foreign Affairs, Commander of the Land Forces, Commander of the Naval Forces Commander of the Air Forces, General Commander of the Gendarmerie. "National Security Council Members", Available at: http://www.mgk.gov.tr/en/index.php/national-security-council/nsc-members (Accessed at: 15/09/2014)

The Council's resolution was that the Secretariat-General of the National Security Council should draft a new National Security Document. The importance of the October 2010 meeting was that cyber threats were for the first time recognised as a global threat by Turkey.[936] Furthermore, since that meeting, Turkish policy-makers have attempted to use global policies such as those of the USA and the UK, in order to stop cyber-attacks. They have also conducted many other cyber exercises in order to learn about any vulnerability among Turkey's official bodies.

6.2.4. The National Cyber Security Exercise of 2011

After the National Security Council meeting, Turkish officials agreed to conduct the second National Cyber Security Exercise in January, 2011. This exercise took place between 25th and 28th January, 2011.[937] In total, 41 public, private and non-governmental organisations participated.[938] The main aim of this exercise was that of "*making a significant contribution to the improvement of administrative, technical and legal cyber security capacity in Turkey, to enhance intra and inter organisational information and experience sharing and to raise awareness at every level, in particular the management level and to determine the organisational competence for computer emergency response.*"[939]

The exercise included two types of attack against chosen cyber systems, including "real attacks" and "written scenarios". Real attacks covered Port Scanning, DDoS Attacks, Website Security Control and Log File Analysis. As mentioned previously, the most significant type of attacks are DDoS attacks (Estonia was devastated by this type of attack in 2007). Written scenarios, on the other hand, included:

- *The unauthorized manipulation of the content of the participant's official website;*

[936] The Secretariat-General of The National Security Council (2010), *27 Ekim 2010 Tarihli Toplantı*, Available at: http://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti (Accessed at: 11/11/2013). Also see, T.C. Cumhurbaşkanlığı (2010), *MGK'da Yeni Milli Güvenlik Siyaseti Belgesi Uygun Bulundu*, Available at: http://www.tccb.gov.tr/haberler/170/77759/mgkda-yeni-milli-guvenlik-siyaseti-belgesi-uygun-bulundu.html (Accessed at: 11/11/2013). Bozkurt, A. (2010), *Siber Savaş Tatbikatı Ertelendi*, Available at: http://www.bilisimdergisi.org/s127/pdf/8-9.pdf (Accessed at: 12/11/2013)

[937] "Ulusal Siber Güvenlik Tatbikatı 2011", Available at: http://www.tk.gov.tr/sayfa.php?ID=28 (Accessed at: 15/09/2014). "Siber Tatbikat Başladı", Available at: http://www.ntvmsnbc.com/id/25175053/ (Accessed at: 15/09/2014)

[938] "Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı", Available at: http://www.btnet.com.tr/17477-ulusal-siber-guvenlik-tatbikati-basariyla-tamamlandi.html (Accessed at: 15/09/2014)

[939] Information and Communication Technologies Authority of Turkey and TUBITAK (2011), *National Cyber Security Exercise 2011 Final Report,* Available at: https://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/ulusal-siber-guvenlik-tatbikati-2011-sonuc-raporu.html (Accessed at: 12/11/2013)

- *The detection of a DDoS attack from an IP address of the participant to another organisation;*
- *The detection of a spam message sent from the IP address of the participant to another organisation;*
- *A DDoS attack on the participant from another source;*
- *A malicious insider's damaging of the participant's database before leaving;*
- *The infection of the participant's systems with a worm that was spread via the Internet;*
- *An attempt at stealing information from the phone of a participant's employee;*
- *An attempt at stealing information from a participant's employee via e-mail;*
- *The detection of a participant's employee attempting to access a site to which access was prevented within the framework of Law No.5651;*
- *The detection of a spam message sent from a fake website that looks as if it belongs to the participant;*
- *The breaking-off of the fibre line connecting the participant to the Internet as a result of an unauthorized excavation;*
- *The break-down of the cooling system in the participant's system control room outside working hours;*
- *The fact that the generator system was not activated despite a power cut in the region of the participant;*
- *The detection of a wireless access point in the participant's premises which could easily be connected to by guessing its name.*[940]

The report revealed the entire participant organisations' and institutions' vulnerabilities with regards to cyber terrorism. According to the Final Report of the exercise, the public institutions, as well as the other organisations, which had participated demonstrated the following disadvantages with regards to fighting against cyber threats:

- *Lack of Information Security Management Systems;*
- *Technical Incompetence of the System Administrators;*

[940] *Ibid.*, pp. 16-17

- *Lack of Intrusion Detection Systems and Processes;*
- *Lack of Awareness about Social Engineering Attacks;*
- *Outdated Antivirus Systems;*
- *Incompetency of System Administrators in terms of Security;*
- *Lack of Intra-Organisational Coordination;*
- *Lack of Access Control Policies;*
- *Ignoring Security at the System Design Stage;*
- *Risks arising from Wireless Networks;*
- *Lack of Business Continuity Plans;*
- *Inability to Detect Port Scan Attacks;*
- *Unfavourable Results from the simulated Distributed Denial of Service (DDoS) Attacks;*
- *Vulnerabilities in the Web Applications;*
- *Inability to Analyse the Log Files Properly.*[941]

Together with the findings of this cyber exercise, the report offered some solutions to resolve these issues, but for the purposes of this paper, the findings of the exercise show that Turkey was open to any cyber-attack. Even though NATO has considered cybercrime a threat since 1999, and has taken serious precautions in order to stop cyber threats, one member nation, Turkey, did not consider cyber threats as a global problem until the mid-2000s. This demonstrates the fact that Turkey had been lax to recognise international organisations' decisions regarding threat perceptions and security.

By evaluating the cyber policy and cyber exercise in terms of Game Theory, interesting results can be deduced. For instance, according to Game Theory, Turkey's cyber infrastructure is not capable of dealing with any cyber threat whatsoever, although both players of the game have to be intelligent and rational. However, the officials' strategies with regards to cyber threats were not in any sense useful. Thus, at this point in time, Turkey could not be accepted as being "intelligent" and, ergo, cannot be considered a viable player of the game. The cyber exercise showed this in a clear way. It would therefore be very easy for cyber terrorists and attackers to have more payoffs from this game. Although Turkey has a weak cyber infrastructure, the cyber exercise was a method it could have used to improve its cyber capabilities. By utilising the findings of the exercise, the country's cyber capabilities

[941] Information and Communication Technologies Authority of Turkey and TUBITAK (2011), *op.cit.*, pp. 19-35

could have been improved, and strong cyber infrastructures erected. Although the cyber terrorists had more of an advantage before this cyber exercise was conducted, since Turkey became more fully informed afterwards, it should have improved its capabilities and balanced this problem. This proved to be a missed opportunity as Turkey was attacked after this particular cyber exercise and many critical, secret documents were stolen by cyber terrorists, it is disappointing that Turkish officials did not heed the findings of the cyber exercise and, ergo, are culpable for not fixing or better defending the country's systems against those threats.

All in all, before the cyber exercise, Turkey's cyber security was weak and vulnerable to cyber terrorist attacks. Game Theory could help officials to improve Turkey's cyber capability in accordance with the exercise findings. This will be explained in the next sub-section.

6.2.5. Cyber Shield Exercise 2012

The Cyber Shield Exercise was conducted in May, 2012[942] with 12 operators having the largest potential in the electronic communication sector in Turkey participating.[943] The aims of that exercise were outlined in the Final Report of the Cyber Shield Exercise 2012 as follows:

- *Be prepared against cyber threats and attacks;*
- *Improve the response capabilities of institutions against cyber incidents;*
- *Enhance the coordination among relevant institutions;*
- *Improve the administrative, technical and legal capacities of cyber security;*
- *Contribute to the sharing of information and experience amongst institutions as well as raising awareness at all levels, especially among IT managers and other executives;*

[942] "National Cyber Shield Exercise 2012", Available at: http://www.icse2014.org/content/national-cyber-shield-exercise-2012 (Accessed at: 15/09/2014). "Siber Kalkan Tatbikatı 2012 Tamamlandı", Available at: http://www.tk.gov.tr/sayfa.php?ID=101 (Accessed at: 15/09/2014). "Türkiye'de Siber Kalkan Koruması", Available at: http://www.turkishny.com/technology/91-technology/90755-turkiyeye-siber-kalkan-korumasi/pdf (Accessed at: 15/09/2014). "Siber Kalkan Açıldı", Available at: http://ekonomi.haberturk.com/teknoloji/haber/746971-siber-kalkan-acildi (Accessed at: 15/09/2014)

[943] TTNET, Turkcell Superonline, Turknet, Gridtelekom, Millenicom, Vodafone, Avea, Dsmart, Türk Telekom, Turkcell, Turksat

- *Emphasize the critical role of internet access providers in cyber security.*[944]

Additionally the document mentioned achieving the following objectives:

- *To test the prevention of illegal traffic (generated by DDoS attacks) by internet access providers before the attacks reach the targeted systems;*
- *To determine the most effective measures for different types of DDoS attacks;*
- *To see the effectiveness of current technological measures and expertise of internet access providers against DDoS attacks;*
- *To assess the coordination capabilities of internet access providers amongst themselves and also with their backbone providers.*[945]

The cyber exercise was conducted using both real attacks and written scenarios. After the exercise, the findings were reported. According to the document, these were:

- *The successful achievement of the exercise regarding both the organizers and the participants;*
- *That DDoS Attacks are preventable;*
- *That DDoS Attacks are preventable at access provider level;*
- *The importance of coordination between access providers;*
- *The importance of preparedness before cyber-attacks happen;*
- *The efficient use of network security tools;*
- *The importance of technical expertise while responding to cyber-attacks.*[946]

Furthermore, the document states that "*DDoS attacks can be prevented with an effective and rapid coordination and accurate countermeasures*."[947] As mentioned in Chapter 1, Estonia faced a DDoS attack at the highest level, with its cyber infrastructure collapsing. At the time, Turkey was still trying to produce its cyber policies, and was not capable of blocking cyber-

[944] Bilgi Teknolojileri ve İletişim Kurumu (2012), *Cyber Shield Exercise 2012 Final Report*, Available at: http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/dokumanlar/Ek10-cyber_shield_2012_final_report_en.pdf (Accessed at: 15/09/2014), p.11

[945] *Ibid*.

[946] *Ibid*., pp. 22-24

[947] *Ibid*., p.6.

attacks or preventing cyber systems from being suddenly overcome by DDoS attacks. The success of Turkey's cyber security policy can be discerned when compared with real cyber-attacks. Turkish officials argue that their systems are able to be tested using cyber exercises in order to identify and fix any of their problems.

To sum up, there has been a visible improvement in Turkey's efforts to build up its cyber security since the 2000s. The exercises outlined above are vital in the sense that they elucidate the disadvantages apparent in Turkey's cyber systems; nevertheless, Turkey still has a long way to go in order to improve its own cyber security.

6.2.6. The Implementation, Management and Coordination of the National Cyber Security Studies

With the increase of cyber-attacks in Turkey, the Council of Ministers ratified the Implementation, Management and Coordination of National Cyber Security Studies in June 2012.[948] According to this document, the Cyber Security Board was established under the presidency of the Ministry of Transport, Maritime Affairs and Communications.[949] The main duty of the Board is that of preparing policies, strategies and action plans for providing the nation with cyber security.[950] The central point about this legislation is that these policies can only be prepared by the Ministry of Transport, Maritime Affairs and Communication, whilst all of the nation's other security institutions and ministries have not been given an opportunity to participate. Turkish officials still demonstrate indifference to cyber threats. In my opinion, if a country is going to attempt to protect itself from cybercrime, the best way of tackling such threats is by ensuring that the necessary policies are prepared by security institutions or the Ministry of Security. Turkey, on the other hand, has selected a very different way of protecting itself from cyber threats (i.e. by making the Ministry of Transport, Maritime Affairs and Communication responsible for drafting such policies). One can only speculate how this policy will affect the country's ability to protect itself from cybercrime. Also, it has to be mentioned here that Turkey is one of the most important members of NATO. Therefore, if Turkish officials were to give the responsibility of drafting their cyber security policies to the nation's security institutions, those institutions would be better able to work and cooperate with NATO staff.

[948] "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Available at: http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (Accessed at: 12/11/2013)
[949] *Ibid.*
[950] *Ibid.*

NATO decided upon its own cyber defence policy in 2011. According to this new policy, "*Recognising that NATO requires a secure infrastructure upon which it can operate, NATO networks, including NATO agencies and NATO missions abroad, will be brought under centralised protection. NATO will also develop minimum requirements for those national networks that are connected to or process NATO information.*"[951] Together with this, the Turkish Armed Forces (TSK) established *The Centre for Cyber Defence* in 2012.[952] The aim of the centre is that of "*defending the nation's own cyber system from any cyber-attack, to intervene every time a cyber-incident occurs, [and] to participate in any cyber exercises performed by the nation and NATO.*"[953] The centre also coordinates between TUBITAK and the Ministry of Transport, Maritime Affairs and Communications. In addition, the centre participated in NATO's cyber exercise of 2012 - indeed, that was the first duty of the centre.[954] Whilst it can be concluded that the official bodies in Turkey are keen to stop cyber-attacks, the coordination of their policies is not reliable. This is because part of the nation's cyber security is run by the Turkish Armed Forces, but there is no specific role for the TSK in deciding the nation's cyber defence policy.

6.2.7. National Cyber Security Exercise 2013

The third national cyber exercise that Turkey participated in was conducted with the coordination between the Ministry of Transport, Maritime Affairs and Communications, the Information and Communication Technologies Authority of Turkey, and TUBITAK between 24th December, 2012 and 11th January, 2013.[955] According to the ICSE2014[956], the main aim of this particular cyber exercise "*was to develop participants' ability to respond to cyber-*

[951] NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence, op.cit.*

[952] Çatal, C. (2013), *TSK'dan Siber Savunma Merkezi,* Available at: http://www.hurriyet.com.tr/teknoloji/22405874.asp (Accessed at: 13/11/2013). "TSK'da Siber Savunma Merkezi Başkanlığı Kuruldu", Available at: http://www.radikal.com.tr/turkiye/tskda_siber_savunma_merkezi_baskanligi_kuruldu-1117859 (Accessed at: 13/11/2013). "TSK Siber Savunma Merkezi Başkanlığı Kuruldu", Available at: http://www.btnet.com.tr/64622-tsk-siber-savunma-merkezi-baskanligi-kuruldu.html (Accessed at: 13/11/2013). Anadolu Ajansı (2013), *TSK'da Siber Suçlarla Mücadele Edecek,* Available at: http://www.aa.com.tr/tr/turkiye/239031--tsk-da-siber-suclarla-mucadele-edecek (Accessed at: 13/11/2013)

[953] "TSK Siber Savunma Merkezi Başkanlığı Kuruldu", *Ibid.*

[954] "TSK'da Siber Savunma Komutanlığı", Available at: http://gundem.bugun.com.tr/tskda-siber-savunma-komutanligi-haberi/215064 (Accessed at: 13/11/2013)

[955] "Ulusal Siber Güvenlik Tatbikatı 2013", Available at: http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2013.php (Accessed at: 16/09/2014). "Siber Güvenlik Tatbikatı Başladı", Available at: http://www.sabah.com.tr/Teknoloji/Haber/2013/01/10/siber-guvenlik-tatbikati-basladi (Accessed at: 16/09/2014). "2. Ulusal Siber Güvenlik Tatbikatı", Available at: http://www.ubak.gov.tr/BLSM_WIYS/UBAK/tr/BELGELIK/guncel_haber/20130110_141118_204_1_2561.html (Accessed at: 16/09/2014)

[956] International Cyber Shield Exercise 2014

attacks, to improve organisational and inter-agency coordination against cyber-attacks and to increase [the] national awareness level of cyber security."[957] A total of 61 public and private sectors participated in this cyber exercise. Seven types of cyber-attacks were imposed by the organizers.[958] Nevertheless, Turkey has been making significant improvements in its cyber security exercises. Although from the first cyber exercise, TR-BOME 2008, to the most recent one, the number of participants has increased, new cyber-attack styles have been utilised - including real cyber-attacks - and the results have often been published to the general public in order to improve the nation's capabilities, it is still not possible to say that the officials, institutions and private sectors actually care about the findings of these exercises. This might be because, from first to last, the same problems were found among all of the participants, such as being vulnerable to the same types of cyber-attacks, communication with the other institutions and improving the cyber infrastructure. The main problem might be the lack of qualified experts, because there has been no clear education on information systems in Turkey. If the public and private institutions cannot find any qualified experts in cyber security, the cyber exercises cannot help states to improve their cyber security.

Lastly, although Turkey has conducted some cyber exercises, there has been no road map to improve cyber security. This is the most significant disadvantage of Turkey's cyber security policy. The Information and Communication Technologies Authority of Turkey and TUBITAK have tried to improve Turkey's cyber security capabilities, but a national road map is also needed to fight against cyber threats.

6.2.8. The Cyber Security Council

The Cyber Security Council was established under resolution of the Council of the Minister. It was published as Law number 28447 in the Official Gazette on 11 June, 2012 and is entitled "The Execution, Management, and Coordination of the National Cyber Security Activities".[959] According to the Official Gazette:

> *"In order to determine the precautions to be taken for cyber security, to approve - and to ensure implementation and coordination of - the plans, schedules, reports, procedures, principles and standards that have been*

[957] "National Cyber Security Exercise 2013", Available at: http://www.icse2014.org/content/national-cyber-security-exercise-2013 (Accessed at: 16/09/2014)

[958] "Ulusal Siber Güvenlik Tatbikatı 2013", *op.cit.*

[959]"Siber Güvenlik Kurulu", Available at: http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/siberguvkurulu.php (Accessed at: 18/09/2014). "Siber Güvenlik Kurulu Kuruldu", Available at: http://www.ntvmsnbc.com/id/25391671 (Accessed at: 18/09/2014)

> *prepared, a Cyber Security Council has been established, which is to be presided by the Minister of Transport, Maritime Affairs and Communications and which is to consist of the undersecretaries of the Ministries of Foreign Affairs, Interior, National Defence, Transport, Maritime Affairs and Communications, including the undersecretaries of Public Order and Security, National Intelligence Organisation, Head of Communication, Electronic and Information Systems of Turkish General Staff, Head of Information And Communication Technologies Authority, Head of The - Scientific And Technological Research Council, Head of Financial Crimes Investigation Council, Telecommunications Communication Presidency and the top managers of the ministries and the public organisations that are to be determined by the Minister of Transport, Maritime Affairs and Communications."*[960]

The first meeting of the Council was on 20 December, 2012.[961] Together with the meeting's resolution, a crucial decision was taken by the members of the Cyber Security Council. According to the resolution of the meeting, the Council decided to put into the action the "National Cyber Security Strategy and Action Plan 2013-2014".[962] In addition, the National Cyber Security Strategy and Action Plan 2013-2014 offered to establish a National Cyber Incident Response Centre (USOM).[963] The aim of the Centre is that of protecting Turkey from any cyber threats.

Furthermore, these sources went on to explain the Turkish cyber security policy in light of these developments: *"The Information and Communication Technologies Authority of Turkey has approved the 'Establishment and Authorization Procedures and Principles of the USOM', dated 22 May, 2013 and numbered 2013/DK-TİB/278."* [964] This resolution document mentions the role of the USOM, which is to respond to cyber incidents according to the

[960] The Ministry of Transport, Maritime Affairs and Communications (2013), *National Cyber Security Strategy and Action Plan 2013-2014*, Available at: http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf (Accessed at: 15/08/2013), pp.6-7. "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", *op.cit.*

[961] Canlı, M. (2013), "Siber Güvenlik", *ASEM Rapor*, Available at: https://issuu.com/asemtr/docs/asem_canli_01 (Accessed at: 15/10/2016), p. 29; BTK (2015), Siber Güvenlik Kurulu, Available at: http://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK-KURULU (Accessed at: 15/10/2016); "Türkiye'nin Siber Güvenlik Politikası", Available at: http://shiftdelete.net/turkiyenin-siber-guvenlik-politikasi-44573 (Accessed at: 15/10/2016);

[962] "2. Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı", Available at: http://www.tk.gov.tr/sayfa.php?ID=153 (Accessed at: 18/09/2014)

[963] Canlı, *op.cit.*, p. 29; Haberleşme Genel Müdürlüğü (2014), *Sektörel SOME Kurulum ve Yönetim Rehberi*, Available at: http://www.udhb.gov.tr/doc/siberg/Sektorel_SOME_Reh.pdf (Accessed at: 16/10/2016), p. 6

[964] I was not able to add the documents as an Appendix due to privacy issues.

national and international studies against cyber threats. Moreover, the centre will also have to coordinate with the other public and private cyber incidents response teams.[965] The main duty of the USOM is to reduce the impact of cyber incidents and to develop new strategies and measures in order to fight against cyber threats.[966] The document does not, however, mention how USOM is to do this. This, therefore, is the main disadvantage of the document.

Together with the creation of the USOM, Turkey has taken on more responsibilities than ever before, but these cyber strategies face problems in terms of identifying the institutional roles which were established with the Action Plan 2013-2014, and those of pre-existing institutions. Moreover, there are no clear descriptions of the potential threats to be found in any document. Officials accept that there are threats at a general level, but it is necessary to identify and explain all potential threats in order to better tackle them. Also, there is another problem for the USOM. Even though the TR-BOME has been established, no classifications of these two key institutions, TR-BOME and USOM, exist in the resolutions and documents. As mentioned above, the USOM and TR-BOME share almost the same responsibilities, but there is no classification of these in the Action Plan 2013-2014.

Returning to the theme of the establishment of the Cyber Security Council, "Additional Article 1" amended Law number 5809, which was published in the Official Gazette on 19 February, 2014.[967] This new regulation made explicit the Cyber Security Council's duties under National Law.[968] After this regulation was accepted, the Cyber Security Council is responsible for confirming cyber security policies, strategies and actions.[969] With the creation of the Cyber Security Council and the USOM, Turkey took another essential step towards improving its national cyber security in 2013, when the National Cyber Security Strategy and Action Plan was passed. As mentioned in the previous sections, it is important for the country to introduce other strategies in order to achieve more gains in terms of Game Theory. With this new Action Plan, Turkey was trying to produce new ideas in accordance with Game Theory. However, some problems occurred when these responsibilities were given to the officials mentioned above.

[965] Article 7 of the "Establishment and Authorization Procedures and Principles of the USOM"

[966] The Ministry of Transport, Maritime Affairs and Communications (2013), *op.cit.*

[967] "Siber Güvenlik Kurulu", *op.cit*. "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun", Available at: http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm (Accessed at: 18/09/2014)

[968] *Ibid*.

[969] *Ibid*.

6.2.8.1. The National Cyber Security Strategy and Action Plan 2013-2014

Although the Council of Ministers ratified the Implementation, Management and Coordination of National Cyber Security in 2012, there was no corresponding strategy and action plan detailing how Turkey was to deal with cyber threats. The National Cyber Security Strategy and Action Plan of 2013-2014 was only accepted in June, 2013. The aims were mentioned in the document as follows:

> *-The cyber security of all of the services, processes and data – and the systems involved in provisioning of these - provided by the public organisations and agencies using information technologies;*
> *-The cyber security of information systems of critical infrastructures which are operated by both the public and private sectors;*
> *-Minimization of the effects of cyber security incidents, determination of strategic cyber security actions to put systems back to their regular operational states as soon as possible following the incidents, and help with better investigation and prosecution of the incident by law enforcement and judicial authorities.*[970]

In addition, according to the Action Plan, the following should be done in order to ensure national cyber security:

> *-Regulatory measures;*
> *-Activities to help with judicial processes;*
> *-Establishing the National Cyber Incidents Response Organisation;*
> *-Strengthening the National Cyber Security Infrastructure;*
> *-Human Resources Education and Awareness-Raising Activities in the Field of Cyber Security;*
> *-Developing National Technologies in the field of Cyber Security;*
> *-Extending the Scope of National Cyber Security Mechanisms*.[971]

For the first time in the history of Turkish cyber security policy, a document had been prepared which mentions in full detail the legal regulations necessary for effective cyber policy. Furthermore, this document shows how the above measures will be carried out, and adjudicates the responsibility to different public and private institutions. Even though other actions and reports had been drafted previously, none of them had any road map for

[970] The Ministry of Transport, Maritime Affairs and Communications (2013), *op.cit.*, p. 10
[971] *Ibid*.

implementing the rules that they outlined. This time, however, the action plan had a road map for implementing the rules stipulated therein; and this is the main difference between this plan and all other previous plans.

An important keystone for the cyber security policy of Turkey is that of establishing the National Cyber Incidents Response Organisation (USOM)[972] which was analysed in the previous section. As mentioned earlier, although the duties of USOM were outlined in the document, it did not clarify the relationship between TR-BOME and USOM. It will affect Turkish cyber security policy in the future if the institutions do not clarify the responsibilities of the two organisations.

Turkey is taking some steps to fight against cyber threats, but officials are still looking for problems at a lower level, because of there not being any evidence which shows cyber terrorism and cyber espionage as being a threat. Although some developments have been made against cyber threats, there is no clear information about how the Action Plan should be continued after it has accomplished all of its aims. In addition, some plans which it outlines have not been completed to date (i.e. October 2016).

6.2.8.2. Teams for Responding to Cyber Incidents (SOME)

One of the most significant aspects of the Action Plan 2013-2014 was that of establishing SOMEs. According to the document:

> *"The National Centre for Cyber Incident Response (USOM), which will be available 7/24 to respond to the threats that may affect the country, will be established, and sectoral "Teams for Responding to Cyber Incidents" (SOME) will be established which are to work under the coordination of the USOM. The sectoral SOMEs will respond to cyber incidents and they will also provide information and hold awareness-raising activities specific to the SOMEs affiliated to themselves and to the sector which they are responsible for. Also other SOMEs will be established within public organisations and agencies which are to operate under the coordination of sectoral SOMEs. The USOM and the SOMEs – while responding to incidents - will also act in coordination with judicial authorities and law enforcement agencies to provide the data that will*

[972] "Siber Saldırılara Müdahale Merkezi Kurulacak", Available at: http://www.ntvmsnbc.com/id/25450250/ (Accessed at: 19/09/2014)

> *support the investigation. As the national contact point, the USOM will be in close cooperation with the equivalent authorities of other countries and international organisations".*[973]

Although SOMEs have the same role in terms of fighting against cyber threats and attacks as TR-BOMEs, SOMEs have been given more responsibility than TR-BOMEs. For instance, SOMEs have the duty of cooperating with other states and international organisations' cyber incidents response teams.

In addition, more information and timescales were provided in the document about reaching the full capacity and responsibility of public and private SOMEs. The document, *"The Establishment, Duties and Studies on the Principles and Procedures Regarding Notification of SOMEs"*, clarifies the responsibilities of sectorial and public SOMEs, and their relationship with the USOM.[974]

With the creation of SOMEs, Turkey should be able to improve its cyber capabilities, but there still exists a problem in terms of implementing the rules stipulated by the Action Plan and other policies. If Turkey wants to improve its capabilities, it is of great import that it applies all rules at the right time.

6.2.8.3. 2016-2019 National Cyber Security Strategy

Following the acceptation of the National Cyber Security and Action Plan 2013-2014, Turkey has tried to improve its cyber security, but as mentioned previously, some of the important decisions of the Action Plan were not due for completion before November 2016. The original Action Plan had covered the years 2013-2014, and therefore the cyber security policy needed a new Action Plan, because technology is improving daily and it is no longer stable. On the other hand, cyber-terrorists are also going to improve their abilities in the international arena.

Although the Ministry of Transport, Maritime Affairs and Communication prepared a draft plan for the National Cyber Security Strategy 2015-2017,[975] this draft plan did not come into

[973] The Ministry of Transport, Maritime Affairs and Communications (2013*), op.cit.*, p. 19

[974] "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ", Available at: http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (Accessed at: 18/10/2014)

[975] Türkiye Bilişim Derneği (2015), "Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu", *Nihai Rapor,* Available at: http://www.kamu-bib.org.tr/wp-content/uploads/2015/10/Kamu-B%C4%B0B-%C3%87G1-Siber-G%C3%BCvenlik-ve-Kritik-Altyap%C4%B1lar.pdf (Accessed at: 16/10/2016), p. 7; "Ulusal Siber Güvenlik Stratejisi ve 2015-2016 Eylem Planı 1 Ortak Çalıştayı Gerçekleşti", Available at: http://sge.bilgem.tubitak.gov.tr/tr/haber/ulusal-siber-guvenlik-stratejisi-ve-2015-2016-eylem-plani-1-ortak-akil-calistayi-gerceklesti (Accessed at: 16/10/2016)

force, and the cyber security policy and action plan of Turkey was interrupted. This was because, according to the Action Plan 2016-2019, during this period several meetings would be held in order to research the security policies of countries, including the USA, Europe and the Far East, in order to adopt important steps in Turkey's cyber security policy.[976]

As a result of these meetings and research, the 2016-2019 National Cyber Security Strategy was prepared by the Ministry of Transport, Maritime Affairs and Communication.[977] According to the document, the Strategy has two main objectives: "*for all stakeholders to acknowledge the understanding that cyber security is an integral part of national security; and secondly, acquiring competency that will allow taking administrative and technological precautions for maintaining the absolute security of all systems and stakeholders in national cyber space*."[978] The important point of the Strategy is that certain cyber security risks are mentioned, and some solutions adopted to reduce the effects of these risks. The risks mentioned are: interruption of critical infrastructure, including energy and transport as the result of cyber-attacks, stealing the identity of citizens, fraud, human errors and natural disasters.[979] These risk perceptions show that Turkish officials and cyber security policy-makers still regard cyber-attacks only in terms of theft, robbery and fraud. Although details of the Estonian cyber-attack were given in Chapter 1, and it is clear that the international community is faced with a new kind of warfare in the form of hybrid warfare/threats, Turkish officials have not evaluated cyber-attacks broadly enough. Also, Turkey has a serious terrorism problem and its neighbours are problematic; therefore the country could face both terrorist attacks and cyber-attacks. It is important to accept the real threat of cyber-attacks, including cyber-espionage and cyber-terrorism. The concept does not consist simply of theft and fraud. Moreover, Turkey has already faced cyber-attacks in its history.

The document offers some solutions to reduce the risks of cyber-attacks, such as creating a critical infrastructure inventory, creating legislation on cyber security, improvement in the level of awareness on cyber security and creating a strong institution or authority for coordination on cyber security, and so on.[980] As can be seen, the creation of legislation on cyber security was mentioned in the first cyber security strategy, the 2013-2014 Action Plan, but the legislation is again mentioned in the new Strategic Plan. This shows us that Turkey's

[976] The Ministry of Transport, Maritime Affairs and Communications (2016), *2016-2019 National Cyber Security Strategy*, Available at: http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf (Accessed at: 17/10/2016), pp. 5-6

[977] *Ibid*.

[978] *Ibid*., p.11

[979] *Ibid*., pp. 18-19

[980] *Ibid*., pp. 20-21

cyber security policy is still behind with the plan, and the document offers timing and dating recommendations to create and organize these solutions.

To sum up, although Turkey has already faced cyber-attacks, when both Strategic Plans are compared, its cyber security policy and the implementation of solutions have not done enough. It is clear that Turkey has a long way to go to improve its cyber security.

Under the next heading, Turkish national law will be discussed in terms of cybercrime and cyber terrorism laws.

6.3. Cybercrime in Turkish National Law

In this section, Turkey's policy on cyber terrorism/attacks will be detailed in terms of the development of its national law, rather than in terms of its public policy, because the Turkish cyber defence policy legislation began with the passing of National Law Number 3756.

The concept of a "cybercrime" was first introduced into the Turkish Penal Code Number 765 with Law Number 3756.[981] Information Technology Crimes with Law Numbers 525/a, 525/b, 525/c and 525/d were also added to the Turkish Penal Code.[982] According to the new law, cybercrime was conceived of in its narrow sense. This means that Turkish officials did not think about cybercrime too much, and did not believe that they could be affected from cyber threats. This might be due to the fact that the Internet and its connections were either too slow or non-existent in Turkey at the time.

The most valuable development in laws regarding cybercrime in Turkey was that of the ratification of Law Number 5237 in 2004 (N.B. the law only officially came into force in 2005).[983] Although cybercrime was covered under the new law, "cyber terrorism" was not actually mentioned. The cybercrime regulation came under the purview of "*Offences in the field of Data Processing Systems*". This regulation covers the following crimes: "*Access to data processing systems,*[984] *hindrance or destruction of the system, the deletion or alteration of data,*[985] *the improper use of bank or credit cards*[986] *and the imposition of security*

[981] 3756 nolu Kanun, *op.cit.*

[982] *Ibid.*

[983] Criminal Code (2004), "Law Number 5237", *Number 25611,* Available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=247129 (Accessed at: 10/11/2013)

[984] ARTICLE 243-(1) Any person who unlawfully enters part or whole of a data processing system or remains there is punished with imprisonment for up to one year, or imposed with a punitive fine.
(2) In case the offences defined in the above sub-section involve systems which benefit against the charge, the punishment to be imposed is increased up to one half. (3) If such an act results in deletion or alteration of data within the content of the system, the person responsible for such failure is sentenced to imprisonment from six months up to two years.

[985] ARTICLE 244-(1) Any person who hinders or destroys the operation of a data processing system is punished with imprisonment from one year to five years. (2) Any person who garbles, deletes, changes or prevents access

precautions on legal entities."[987],[988] In addition, the new law also punished ICT-mediated crimes. This was the first time Turkish officials had tried to take control of information crimes in the broader sense. For instance, Article 124 of Law Number 5237 deals with the Prevention of Communication,[989] Article 125 deals with Defamation,[990] Article 132 organises lawful resolutions against the Violation of Communicational Secrecy,[991] Article 133 regulates

to data, installs data in the system, or sends the available data to other places is punished with imprisonment from six months to three years. (3) The punishment to be imposed is increased by one half in the case of commission of these offenses on the data processing systems belonging to a bank or credit institution, or public institutions or corporations. (4) Where the execution of above mentioned acts does not constitute any other offence apart from unjust benefit secured by a person for himself or in favour of third parties, the offender is sentenced to imprisonment from two years to six years, and also imposed with a punitive fine of up to five thousand days.

[986] ARTICLE 245-(1) Any person who acquires or holds bank or credit cards of another person(s) whatever the reason, or uses these cards without consent of the card holder or the receiver of the card, or secures benefit for himself or third parties by allowing use of the same by others, is punished with imprisonment from three years to six years, and also imposed with a punitive fine. (2) Any person who secures benefit for himself or third parties by using a counterfeit bank or credit card is punished with imprisonment from four years to seven years if the act executed does not constitute any offence other than forgery.

[987] ARTICLE 246-(1) Security precautions specific to legal entities are imposed in case of commission of the offences listed in this section within the frame of activities of legal entities.

[988] *Ibid*; Also See; Dülger, M. V. (2005), *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, Available at: http://www.dulger.av.tr/pdf/bilisimsuclariveyctk.pdf (Accessed at: 10/05/2014)

[989] ARTICLE 124-(1) In case of unlawful prevention of communication among the persons, the offender is sentenced to imprisonment from six years to two years or imposed punitive fine.
(2) Any person who unlawfully prevents communication among the public institutions is punished with imprisonment from one year to five years.
(3) Punishment is imposed according to the provisions of the second sub-section in case of unlawful prevention of broadcasts or announcements of all kinds of press and publication organs.

[990] ARTICLE 125- (1) Any person who acts with the intention to harm the honour, reputation or dignity of another person through concrete performance or giving impression of intent, is sentenced to imprisonment from three months to two years or imposed with a punitive fine. In order to punish the offence committed in absentia of the victim, the act should be committed in the presence of least three persons.
(2) The offender is subject to the above stipulated punishment in case of commission of offence in writing or by use of audio or visual means directed at the aggrieved party.
(3) In case of commission of offence with defamatory intent:
a) Against a public officer,
b) Due to disclosure, change or attempt to spread religious, social, philosophical belief, opinion and convictions and to obey the orders and restriction of the one's religion,
c) By mentioning sacred values in view of the religion with which a person is connected, the minimum limit of punishment may not be less than one year.
(4) The punishment is increased by one sixth in case of performance of the defamation act openly; if the offence is committed through the press and use of any one of publication organs, then the punishment is increased up to one third.
(5) In case of defamation of public officers working as a committee to perform a duty, the offence is considered to have been committed against the members forming the committee.

[991] ARTICLE 132-(1) Any person who violates secrecy of communication between the parties is punished with imprisonment from six months to two years, or imposed with a punitive fine. If violation of secrecy is realized by recording of the contents of communication, the party involved in such an act is sentenced to imprisonment from one year to three years.
(2) Any person who unlawfully publicizes the contents of communication between persons is punished with imprisonment from one year to three years.
(3) Any person who openly discloses the content of the communication between himself and others without obtaining their consent, is punished with imprisonment from six months to two years,
(4) The punishment determined for this offence is increased by one half in the case of disclosure of contents of communication between the individuals through press and broadcast.

the Tapping and Recording of Conversations between Individuals,[992] Article 135 concerns the Recording of Personal Data,[993] Article 136 arranges rules of law against the Unlawful Delivery or Acquisition of Data,[994] Article 138 organises stipulations against the Destruction of Data,[995] Article 142 regulates Qualified Larceny,[996] Article 158 regulates Qualified forms of Fraud,[997] and Article 226 organises regulations against Indecency.[998] These Articles

[992] ARTICLE 133-(1) Any person who listens to non-general conversations between the individuals without the consent of any one of the parties or records these conversations by use of a recorder, is punished with imprisonment from two months to six months.
(2) Any person who records a conversation in a meeting not open to the public without the consent of the participants by use of a recorder, is punished with imprisonment up to six months, or imposed with a punitive fine.
(3)Any person who derives benefit from disclosure of information obtained unlawfully as declared above, or allowing others to obtain information in this manner, is punished with imprisonment from six months to two years, or imposed with a punitive fine up to thousand days.

[993] ARTICLE 135-(1) Any person who unlawfully records the personal data is punished with imprisonment from six months to three years.
(2) Any person who records the political, philosophical or religious concepts of individuals, or personal information relating to their racial origins, ethical tendencies, health conditions or connections with syndicates is punished according to the provisions of the above subsection.

[994] ARTICLE 136-(1) Any person who unlawfully delivers data to another person, or publishes or acquires the same through illegal means is punished with imprisonment from one year to four years.

[995] ARTICLE 138-(1) In case of failure to destroy the data within a defined system despite expiry of legally prescribed period, the persons responsible for this failure are sentenced to imprisonment from six months to one year.

[996] ARTICLE 142-(1) In case of commission of offence of larceny;
a) In public institutions and corporations no matter who is the owner, or in places reserved for worship or by stealing the property used in the public interest or services,
a) By stealing the property under custody in public places or buildings or their attachments,
b) By stealing the property in the transportation vehicles provided for public use, or in arrival/departure terminals,
c) By stealing the property reserved for prevention of damages likely to be caused by a disaster or mitigation of its affects,
d) By stealing the property left in a certain place for use upon requirement,
e) By unlawful use of energy, the offender is sentenced to imprisonment from two years to five years.
(2) In case of commission of this offence;
a) Against a person who is incapable to protect his belongings, or by taking advantage of a death,
b) By taking away the property carried on with a special skill,
c) By taking advantage of the fear or panic resulting from a natural disaster or social events,
d) By unlocking a door or safe with a counterfeited key kept unlawfully,
e) By use of data processing systems without consent,
f) By trying to conceal his identity or showing himself as a public officer although he is not authorized to do so,
g) By lifting cattle kept in shelters, herds or open places, the offender is sentenced to imprisonment from three years to seven years. In case of commission of offence against a person who cannot defend himself due to corporal or spiritual disability by executing the acts mentioned in paragraph
(b) of this subsection, the punishment to be imposed is increased up to one third.
(3) In case of commission of this offence by breach of rules relating to liquefied energy or any kind of energy in the form of gas, the punishment is determined in consideration of provisions of the second sub-section. In case of commission of this offence within the frame of activities of an organized group, the offenders are sentenced to imprisonment up to fifteen years and also imposed with a punitive fine up to ten thousand days.

[997] ARTICLE 158-(1) In case of commission of offence of fraud;
a) By exploiting religious belief and perception of a person,
b) By taking advantage of his being in a risky or difficult condition,
c) By taking advantage of gradual deterioration of consciousness of a person,
d) By using public institutions and corporations, public professional organisations, political parties, foundations or associations as a tool,

illustrate that Turkey was still viewing cybercrime in its narrow sense, because there is no clear information about how these legislations are supposed to be implemented. Also, when Turkey accepted this law, no policies existed at the time regarding cybercrime. This situation would create a disadvantage for Turkish policy-makers in terms of implementing these legislations. Another important negative point about this law is that it failed to classify cybercrimes, e.g. cyber terrorism and cyber espionage. Although Turkey has a terrorism problem, officials have not accepted terrorist activities performed on the Internet as a crime. This is a huge drawback of the new Turkish law.

Turkey also accepted Article 134 of the Turkish Criminal Procedures Code in 2004 which related to cybercrime. This law does not directly regulate on cybercrime, but it does give

e) By executing acts to the disadvantage of public institutions and corporations,
f) By using data processing systems, banks and financial institutions as an tool,
g) By benefiting from the facilities of press and publication organs,
h) By executing fraudulent acts within the frame of trading activities of the persons being a merchant or executive of a company, or of those acting on behalf of the company,
i) Through breach of trust by the free-lancers,
j) By extending a loan which is not allowed by the bank or any other finance institution,
k) With the intention of collecting insurance money, the offender is punished with imprisonment from two years to seven years and imposed with a punitive fine up to five thousand days.
(2) Any person who secures benefit for others through fraud by mentioning that he has good relations with public authorities and also influence upon them, and deceives a person by promising to perform a certain work, is punished according to the provisions of the above sub-section.

[998] ARTICLE 226-(1) Any person involved in an unlawful act;
a) By allowing a child to watch an indecent scene or a product, or to hear shameful words,
b) By displaying these products at places easy to reach by children, or reading the contents of these products, or letting other to speak about them,
c) By selling or leasing these products in such a way as is open for public review,
d) By selling, offering or leasing these products at places other than the markets nominated for sale of these products,
e) By gratuitously supplying or distributing these products along with other goods or services,
f) By making advertisement of these products, is punished with imprisonment from six months to two years.
(2) The persons who publicize indecent scenes, words or articles through press and broadcast organs or act as intermediary in publication of the same is punished with imprisonment from six months to three years.
(3) Any person who uses children in production of indecent scenes, words or articles is punished with imprisonment from five years to ten years, and also imposed with a punitive fine up to five thousand days. Any person who engages in import, duplication, transportation, storage, export of these products, or presents the same for other's use, is punished with imprisonment from two years to five years, and also imposed with a punitive fine up to five thousand days.
(4) Any person who produces products containing audio-visual or written material demonstrating abnormal sexual intercourse by using sex, with animals, or with the body of a death person, and engages in import sale, transportation storage of the same and presents such material for other's use, is punished with imprisonment from one year to four years.
(5) Any person who publicizes the contents of the products mentioned in the third and fourth sub-sections through press and broadcast organs, or acts as intermediary in publication of the same, or lets children read, hear or see this material is punished with imprisonment from six months to ten years, and also imposed with a punitive fine up to five thousand days.
(6) Security precautions specific to legal entities are imposed due to such offences.
(7) Excluding the third sub-section, the provisions of this article may not be applicable for works of art which are produced for scientific, artistic or literary purposes in order to avoid children to reach such material.

public prosecutors the responsibility to find evidence about the crime. Article 134 of the Turkish Criminal Procedures Code regulates this responsibility for the public prosecutor.[999]

After these developments, Turkey accepted Law Number 5651 entitled the "Regulation of Publications on the Internet and Suppression of Crimes Committed" in 2007.[1000] According to Akdeniz,

> *"The enactment of this law followed concerns for the availability of defamatory videos involving the founder of the Turkish Republic Mustafa Kemal Atatürk through YouTube, combined with increasing concerns for the availability of child pornographic, obscene, and Satanist content on the Internet, and websites which provide information about suicide, or about illegal substances deemed harmful or inappropriate for children. The Telecommunications Communication Presidency (TIB) was chosen as the organisation responsible for executing blocking orders issued by the courts, and has been given authority to issue administrative blocking orders with regards to certain Internet content hosted in Turkey, and with regards to websites hosted abroad in terms of crimes listed in Article 8.*"[1001]

All of these arrangements only cover cybercrimes conducted over the Internet, including pornography and other videos. Turkey has not paid any attention, however, to cyber terrorism. Bıçakçı mentions, with regards to this situation, that "*even attacks which are serious on the significant security institutions were discussed within the framework of the fight against terrorism.*"[1002]

Together with these new arrangements, many websites were blocked in accordance with illegal services. At the same time, three new regulations[1003] were published by the Prime Minister in accordance with the subject of Law Number 5651.[1004] Although there were some

[999] "Turkish Criminal Procedures Code", Available at: http://www.justice.gov.tr/basiclaws/cmk.pdf (Accessed at: 19/09/2014), p. 140

[1000] 5651 nolu Kanun (2007), *Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, Available at: http://www.tbmm.gov.tr/kanunlar/k5651.html (Accessed at: 15/11/2013)

[1001] Akdeniz, Y. (2009), *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship*, Available at: http://ec.europa.eu/enlargement/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censorship.pdf (Accessed at: 09/11/2013), p.4

[1002] Bıçakçı, S. (2013), *21. Yüzyılda Siber Güvenlik*, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, p.45

[1003] These are: 1) Regulations Governing the Access and Hosting Providers on 24 October 2007. 2) Regulations Governing the Mass Use Providers on 01 November 2007.3) Regulations Governing the Internet Publications on 30 November 2007. The details can be found in Akdeniz, *op.cit.*, p.6

[1004] Akdeniz, *Ibid.*, p.6

new developments, these did not impede cyber-attacks. In 2010 and 2011, there were many attacks on official websites because of the new regulations about the blocking of websites.[1005] For example, information was stolen from the Board of Higher Education and the Turkish Ministries of Justice and the Interior in 2012,[1006] thus demonstrating that Turkey has to improve its laws and security with regards to cyber security.

Furthermore, even though Turkey signed the Council of Europe Convention on Cybercrime in November 2010, [1007] the Convention was only ratified with Reservations and Declarations[1008] by the Grand National Assembly of Turkey in 2014 under Law Number 6533.[1009] With the ratification of the Convention, the Turkish Penal Code with regards to cybercrime will be rearranged in accordance with the Convention's laws.

Returning to cyber terrorism, there is no information about cyber terrorism in the Turkish Penal Code and Turkish National Law. Turkish officials evaluate cyber terrorism under the Anti-Terror Law. Turkey accepts that if activities were committed for terrorist aims, they would be evaluated under Article 4 of the Anti-Terror Law. Part of Article 4 of the Anti-Terror Law states that:

> "*Offences Committed for Terrorist Purposes*
>
> *In applying this law offences defined in:*
>
> *a) Articles 79,80,81,82,84,86,87,96,106,107,108,109,112,113,114,115,116,117,118,142,148,149,151,152,170,172,173,174,185,188,199,200,202,204,210,213,214,215,223,224,243,244,265,294,300,316,317,318, and 319*[1010] *with the second paragraph of Article 310 of the Turkish Penal Code."*[1011]

[1005] Kalafat, H. (2011), *Yeni Bir Tip Savaş: Siber Saldırı ve Anonymous Örneği*, Available at: http://yenimedya.wordpress.com/2011/06/15/yeni-bir-tip-savas-siber-saldiri-ve-anonymous-ornegi/ (Accessed at: 10/11/2013)

[1006] "Türkiye'ye Siber Saldırı", Available at: http://www.hurriyet.com.tr/teknoloji/20440458.asp (Accessed at: 15/11/2013).

[1007] "Türkiye de "Sanal Suçlar Sözleşmesini "İmzaladı", Available at: http://www.bilisimdergisi.org/s127/pdf/10-13.pdf (Accessed at: 12/11/2013). "Turkey Logs on to Europe's Internet Treaty", Available at: http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkey-signs-cybercrime-convention-promises-international-cooperation-2010-11-10 (Accessed at: 12/11/2013)

[1008] Başbakanlık (2012), *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı,* Available at: http://www2.tbmm.gov.tr/d24/1/1-0676.pdf (Accessed at: 20/09/2014), pp. 6-7

[1009] Bakanlar Kurulu Kararı (2014), *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun,* Available at: http://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm (Accessed at: 20/09/2014)

[1010] "Turkish Criminal Procedures Code", *op.cit.*.

[1011] "Terörle Mücadele Kanunu", Available at: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf (Accessed at: 21/09/2014)

Although Turkey accepts these rules of law for terrorist activities, it does not classify the terrorist organisations it wishes to specifically target. Thus, Turkey is still evaluating all terrorist activities under the more general heading of counter-terrorism.

In addition, Turkey signed and ratified the International Convention for the Suppression of the Financing of Terrorism and the United Nations Security Council Resolutions 1267 (1999), 1988 (2011) and 1989 (2011) in 2013.[1012] [1013]

Furthermore, Turkey has also participated in projects for improving the capacity of its justice system. In accordance with these projects, Turkey has played another strategy of Game Theory against cyber threats. For instance, it participated in the Council of Europe IPA Project[1014] in order to improve its justice system. The main aims of the IPA project are: *creating cybercrime policies and strategies, the harmonisation of legislation, international cooperation, law enforcement training, judicial training, financial investigation and cooperation between law enforcement and internet service providers.* [1015] With the IPA project, the coordination between policy-makers and law enforcement officers will be improved and Turkey will achieve an international level of legislation. This means that it will have equal legislations to the international community. Turkey has also participated in the Twinning Project.[1016] The aims of project are as follows:

> "*…the revision of Turkish Legislation and to [make compatible] the Turkish National Law with the Convention on Cybercrime, the preparation of the required training modules for law enforcement and judicial authorities, to improve the cooperation between law enforcement and internet service providers and to improve international cooperation.*"[1017]

To sum up, Turkey has some rules of law for fighting cybercrime, but these are not sufficient for fighting against information crimes. The reluctance to classify crimes will be seen in

[1012] Bakanlar Kurulu Kararı (2013), *2013/5428 SAYILI KARARNAMENİN EKİ*, Available at: http://www.resmigazete.gov.tr/eskiler/2013/10/20131010-1.htm (Accessed at: 20/11/2013)

[1013] The ratification of the UN resolutions were about people, some organisations and institutions' which supports the terrorist organisations, properties, monies and other wealth freeze by Turkish government.

[1014] More information about the Cybercrime IPA is Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp

[1015] "Project on Regional Cooperation against Cybercrime in South-Eastern Europe", Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Project_Summary_(Cybercrime_IPA)_dec_12.pdf (Accessed at: 22/09/2014)

[1016] More information about the project is available at: http://ec.europa.eu/enlargement/tenders/twinning/index_en.htm

[1017] ICC Turkey (2011), *Promoting and Protecting Intellectual Property in Turkey*, Available at: http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/International-engagement-and-Advocacy/Country-Initiatives/Turkey/ (Accessed at: 15/07/2016)

Turkey in the same way as other countries and international organisations, but it is necessary to define and identify all kinds of threats in the nation's law. In addition, Turkey needs to sign and ratify international agreements, and keep its word, in order to better fight against cyber terrorism and cyber threats.

6.4. The Application of the Game Theory to Turkey's Cyber Defence Policy

The Game Theory was explained in depth earlier on, in Chapter 3, but a little bit of information will be given here as a reminder of its aim. The main aim of the Game Theory is a decision-making rule to minimize the maximum possible loss, or maximize the minimum gain in a game. Political or economic interests, struggles and strategies can be used instead of the game. Both sides of the game, politics, or attackers and defenders would like to have more gain or effect in the strategy, and therefore they do their best to achieve this aim. Both sides must be rational and intelligent in the game in order to have more gain.[1018] As mentioned above, both sides must be rational and intelligent to be able to produce new strategies to realise their aims. Rapoport mentions this situation in his work as:

> *"Each player would need to develop new ways in order to obtain more outcomes against his or her opponents; this means that each player should strategically think about the next step of his or her moves; furthermore, the player should calculate how his or her payoffs will impact the other players of the game."*[1019],[1020]

Having recalled some of the details of Game Theory, Turkey's policy can be evaluated under the theory. Even though some interpretations have already been posited in the chapter, I would like to again mention that Turkey's cyber security policy after the Cold War was non-existent until it began producing policies again. As mentioned previously, the country's lack of intelligence was largely due to officials not having any strategy, plan, or idea about the threat, as they did not have any information about cyber systems, but Turkey accepted its first cyber security strategy and action plan in 2013 to improve its cyber infrastructure security.

Nevertheless, if it is still possible to say anything more in terms of this theory, the first time Turkey introduced cyber security can be explained as being a Zero-Sum fraction game. I will use the following table to explain this situation.

[1018] Neel, *op.cit.*, pp. 69–72. *Also see,* Poundstone, *op.cit.*, p.44

[1019] Rapoport (1974), *op.cit.*, p. 86

[1020] See Chapter 3 for more details

		Cyber-Terrorists	
		Attack	Do no Attack
Turkey	High	4, -4	-3, 3
	Low	-5, 5	4, -4

Table 19: Zero-Sum game for NATO's Cyber Security Policy

The table illustrates the expected payoff distribution between Turkey and Cyber-Terrorists. Both sides have two different strategies in the game: Turkey is able to choose high level or lower level cyber security policies, and on the other side, cyber-terrorists can choose attack or do not attack. High level security policy can be more expensive than lower level policies, but nevertheless reduces the success rate for cyber-terrorists, and high level cyber security policies require more attention and information. The game does not have any pure Nash Equilibrium, and the total of the payoffs are Zero-Sum. This is because, as stated previously, Turkish officials still evaluate cyber security policies in terms of online theft, fraud and stealing of identities. Furthermore, there was no effective policy for fighting cyber-attacks without fraud, theft and stealing identities. Also, cyber security strategies have not been supported by a definition of the concepts and legislation, which has missed out cyber security strategies. Therefore, Turkey incurred maximum losses, and the cyber terrorists obtained maximum gains at this time. In sum then, the Zero Sum Game fraction was formed.

According to the table, the current situation of Turkey's cyber security policy, can be explained as: although Turkey has researched and investigated other countries' cyber security policies, it seems clear that the other types of cyber threats, cyber espionage and cyber-terrorism have not been accepted as a threat in Turkey, and that Turkey plays the lower level security policy. On the other side, cyber-terrorists choose to play an attack on Turkey's cyber infrastructure to maximize their payoff. With the chosen strategies, Turkey will have payoff of -5, and the cyber-terrorists will have payoff of 5, and the total is 0.

As can be seen from the table, if Turkish officials used a Game Theory to determine expected payoff with regards to the level of cyber security strategy, then Turkey could have more payoff than the cyber-terrorists. The Game Theory can help Turkey, and other states and international organisations to maximize their payoffs or advantages against other groups, such as terrorist groups, and offers important solutions to resolve any dispute. Similarly, some examples were given in Chapter 3 of the use of Game Theory in the Cold War era to solve the nuclear arms race and Cuban missile crisis. Therefore the theory can be used to analyse cyber security policies and strategies in terms of expected situations and payoffs before coming into force officially.

In the next section, the cyber policy will be evaluated, and I will offer some recommendations for stronger cyber security. As stated in the introductory part of this chapter, the main aim is to analyse and evaluate the cyber security policy and offer some recommendations to Turkish officials. Therefore the next heading is most valuable to ensure compliance with this aim.

6.5. Assessment and Recommendations

6.5.1. Assessment

In this chapter, Turkey's cyber security policy has been detailed and some key points about the policy have been emphasised in terms of the country's historical background and national law. Although Turkey has improved its cyber security capabilities by accepting security policies and establishing new bodies, it still has a long way to go in order to completely improve these capabilities.

There is no doubt that Turkey has a lot of vulnerability in terms of cyber threats. The most significant disadvantage of Turkey's cyber policy is that, although a plan may exist, it cannot be completed in time, e.g. the Action Plan having been published one year after the "Implementation, Management and Coordination of the National Cyber Security" was implemented. Although the Convention on Cybercrime was signed in 2010, it was only ratified in 2014. These events can be taken as examples of Turkey's vulnerabilities.

Turkey must be wary of other kinds of terrorism as well, but up until the present time, it has been evaluating terrorism in its outdated guise (i.e. not including cyber terrorism under that term's auspices). An illustration of this is the country's ratifying new laws which evaluate terrorism only under its narrow sense. If Turkey wants to have legislations which are in accordance with international law, it will first have to change its Anti-Terror Law by defining and identifying other kinds of terrorist activities.

Also, one of the other problems in the cyber security policy of Turkey is that Turkish officials have given the responsibility of developing the nation's cyber security to the Ministry of Transport, Maritime Affairs and Communications. Guaranteeing the nation's security is more important than the issues which that ministry specialises in. Cyber security needs more concentration and information than other duties. In my opinion, this responsibility should instead be allotted to the Prime Ministry, because it coordinates the other ministries and institutions better than the Ministry of Transport, Maritime Affairs and Communications. Moreover, the Prime Ministry is more powerful than the Ministry of Transport, Maritime Affairs and Communications. In addition, other critical security institutions, such as the National Intelligence Organisation, the Turkish Armed Forces and the Republic of Turkey's Secretariat-General of the National Security Council, depend on the Prime Ministry. As Dowding states that "*prime ministers are more powerful within their systems*[1021] *...all ministers are powerful within their own domain*"[1022] and therefore the best way to prepare cyber security policies is by the Prime Ministry, because the Prime Ministry will coordinate all Ministries and institutions better than other organisations; also, the Prime Minister is the Head of the Government. Turkish officials have *to think* from this point-of-view in order to develop the nation's security policy.

Turkey has conducted some cyber exercises in order to identify its vulnerabilities with regards to cyber-attacks, and for the purpose of improving its cyber infrastructure. Although its first cyber exercise took place in 2008 under the auspices of TR-BOME, Turkey's cyber security still faced the same problems up until 2014 with regards to conducting other cyber exercises (e.g. analysing different types of cyber-attacks, communicating with other institutions and improving its cyber infrastructure, protecting the cyber infrastructure of its institutions, resolving password problems, etc.). In addition, cyber-attacks have shown the vulnerabilities of Turkey in cyberspace to the international community.[1023] This situation has created despair in terms of improving the cyber capabilities of Turkey. I believe that Turkey can improve its cyber capabilities, but this would require more qualified and knowledgeable staff. Therefore, it must try to educate its personnel before trying to fight against cyber threats. The cyber exercises that the country has conducted have clearly demonstrated this problem to the officials.

To sum up, in my opinion, although Turkish policy-makers mention Turkey's cooperation with other countries and organisations, they do not care about these policies sufficiently

[1021] Dowding, K. (2013), "The Prime Ministerialisation of the British Prime Minister", *Parliamentary Affairs*, Vol. 66, p. 617

[1022] *Ibid*., p. 622

[1023] "Türk Bankaları Siber Saldırı Altında", Available at: http://www.hurriyet.com.tr/teknoloji/27037274.asp (Accessed at: 10/10/2014); "Türkiye'ye en çok bu 3 ülkeden siber saldırı geliyor", Available at: http://www.hurriyet.com.tr/teknoloji/26989400.asp (Accessed at: 10/10/2014). "Türkiye'ye 6 ülkeden siber saldırı", Available at: http://www.yenisafak.com.tr/gundem/turkiyeye-6-ulkeden-siber-saldiri-635531 (Accessed at: 10/10/2014); "Almanlar'dan Hazine'ye Siber Saldırı", Available at: http://www.yenisafak.com.tr/gundem/turkiyeye-6-ulkeden-siber-saldiri-635531 (Accessed at: 10/10/2014) because, firstly, cyber security policies have to be prepared by the country's security services under the auspices of the Prime Ministry, not the Ministry of Transport, Maritime Affairs and Communication. Secondly, national and international cooperation is essential for deciding what other steps should be taken in order to protect Turkey from cyber threats. Furthermore, and above all, Turkey needs to accept and explain these new threats within the Turkish Penal Code.

6.5.2. Recommendations

As already mentioned, Turkey started to take significant measures to combat cyber threats in the mid-2000s, and can be said to be at the early stage of taking the issue seriously. Therefore I will now make a few recommendations for Turkey to follow in respect to combating cyber terrorism.

The first step in the fight against cyber threats is that of preparing a document to classify critical cyber infrastructures, which would also reveal any weak aspects of the infrastructure. It will then be possible to plan further steps towards guaranteeing cyber security policies and improving the capabilities of the country's cyber infrastructure.

The second step towards establishing an effective cyber security policy is that of preparing a corresponding strategy. This will be similar to the Action Plan 2013-2014, but this plan must also include alternative strategies for fighting against cyber threats.

The third step would be that of defining all threats separately and explaining them in official documents. Together with these definitions and explanations, the officials and security agents will also have to decide on effective solutions against the threats.

The fourth step in the fight against cyber threats is that of translating all such threats into Turkish national law. This is because Turkish law has not covered all threat perceptions in its Penal Code along with its other policies. For instance, there is no information available about the concept of cyber terrorism in Turkey. Furthermore, some cases, such as cyber terrorist activities, need to be evaluated under Anti-Terror Law. Therefore, Turkey must implement and explain all concepts and threats in order to make better decisions in the future.

Fifthly, separate arrangements should be made for all types of crimes, and the law should not be missing any of the parties. As mentioned above, Turkey does not have separate laws for different kinds of crime. With the current arrangement, laws may be applied in a more relaxed way to cybercrime.

Furthermore, although the Action Plan covers the search and implementation of international law to the National Penal Code or Turkish National Law, Turkey has not conducted enough research on cyber threats at the national and international levels in order to examine other states' and international organisations' rules. For instance, although Turkey signed the Convention on Cybercrime in 2010, it was only ratified by the nation in 2014. There is a big gap between signing and ratifying international law in Turkey. This will create a huge problem for Turkey in the future, as there will continue to be gaps between it and other countries. Turkey must apply such regulations to its own cyber law quickly, because the threat is still great, and may be more dangerous for Turkey in the coming era.

Hence, it is of great importance that Turkey cooperates with other countries in order to stop cyber terrorism. Specifically, Turkey has to cooperate with other countries' cybercrime departments, private sectors and other critical institutions, such as intelligence agencies, in order to learn more about their policies and alternative ways of preventing cyber terrorist activities. Cooperation is also valuable in terms of catching the cyber terrorists as well.

The eighth suggestion for achieving an effective cyber security policy is that of signing bilateral and multilateral agreements in order to improve cooperation with other states and international organisations. However, it is not enough simply to sign bilateral and multilateral agreements. They also have to be ratified and implemented on a national level as well.

Also, it is crucial and necessary to educate individuals about the different perceptions of cyber threats. Together with the rising awareness of such information, individuals should improve their cyber infrastructure at home.

Lastly, significant institutions' information systems, including those of Ministries, should be collected in a centre which will be established, or using pre-existing institutions for this aim, and all information should be recorded. In addition, the public should agree to give total authority to this centre in the case of any sudden cyber-attack. For this, the cyber centre's staff should be fully equipped in terms of knowledge, and has to be able to manage any cyber-attack whatsoever. For that reason, exchanging personnel with other states for training is essential. They would accordingly learn more about other states' cyber security policies; and this will, in turn, help to improve the cyber capabilities of Turkey.

To sum up, Turkey must follow these recommendations in order to improve its cyber security capabilities. As was mentioned in the previous sections, Turkey has a complex bureaucracy and, if it employs this bureaucracy in cyber security decisions, in my opinion, Turkey will not be able to improve its cyber security policy. This is due to the fact that, because cyberspace is so vast, it would be impossible to take control of it. Moreover, since cyber terrorists are constantly improving their techniques and capabilities, Turkey will have to make fast decisions and implement them at a moment’s notice in order to protect itself from cyber-attacks.

6.6. Conclusion

As detailed above, Turkey is still at the early stages of producing and implementing cyber security policies (vis-à-vis other NATO countries). The first internet connection was made in 1986, and the first public usage of the Internet was in 1993.[1024] Nevertheless, whilst the public was first allowed to use the Internet in 1993, Turkey had passed a law (#3756) in 1991 which attempted to regulate the Internet. One could accept this as prescience, but today, Turkey is still at the same level in terms of producing such laws.

Of course, privacy is crucial with regards to security policies, but it is also necessary to help researchers to know more about cyber security policies. This exchange of information is really salient for the purpose of improving the country’s cyber security capabilities. Therefore, Turkey, NATO, and other states must cooperate with researchers for the purpose of improving their mutual cyber security.

From the point of Game Theory, before the accepting any cyber security policy, it is crucial to analyse and determine expected payoffs. As detailed in the previous sections, Turkey did not have qualified cyber security personnel, thus creating a negative point for Turkey. If Turkey would like to have more gains in the cyber security game, it must improve the quality of its cyber security personnel.

All in all, Turkey’s cyber policy is not yet sufficient enough. There are many aspects which require improvement, which have been mentioned in the recommendations part of this chapter. Quality policy is made by quality personnel who, in turn, are supported by quality legislations. I believe that Turkey will eventually hire quality personnel on cyber research and will improve its cyber security policies, but I cannot believe that it will improve its justice system with its current form of bureaucracy. If Turkey can solve this problem, it could have important cyber security policies, although I believe that such policies can never entirely prevent all cyber-attacks. What is needed is to change the country’s mind-set with regards to fighting cyber threats. If Turkish officials think that cyber threats or cyber terrorism is the same as counter-terrorism, this problem will not be solved in the near future. Therefore, the country must change its mind-sets and face its problems in order to resolve them.

[1024] “Dünya’da İnternet’in Gelişimi”, Available at: http://www.internetarsivi.metu.edu.tr/tarihce.php (Accessed at: 22/09/2014)

Since Turkey has taken some steps for the purpose of solving terrorism problems after 30 years, I hope that officials nowadays will care more about cyber threats.

CHAPTER 7: CONCLUSION

As mentioned at the beginning of the thesis, this research is centred on some questions, one of the main questions being why the Estonian Case is important for the international community and how it has affected states and regional/international organisations policies, particularly NATO. The thesis is also essentially based on one legal question, which is the development of the application of international law against cyber-attacks. Through analysing and evaluating the process of cyber security policies and the application of international law against cyber-attacks, there was clearly a lack of information on the cyber threat and its effects until the case of Estonia.

In the first chapter, the importance of the Estonian case was detailed, showing how it acted as a catalyst for improvements in the cyber security systems of states and international organisations. The international community has experienced many cyber-attacks, NATO facing its first attacks in 1999, but the organisation did not produce effective policies until it was forced to confront the Estonian cyber-attacks. Although it has implemented some policies in the establishment of the NCIRC, NATO has only taken important steps on cyber security since the case of Estonia. This situation is supported by the view of Laasme.[1025] This series of cyber-attacks opened the eyes of NATO, and the organisation has made the important decision to protect itself and its Allies from cyber-attacks. The accreditation of the CCD COE and the establishment of the CDMB are important in determining future policies on cyber security, because CCD COE is the education, research and development centre on cyber security and researches and exercises new policies on cyber security. CDMB is the coordinating body in NATO, and helps its Allies to improve their cyber securities. These institutions were established and accredited after the Estonian attacks, which, again shows us the importance of the Estonian case.

The Estonian case also revealed the problem of the application of international law and the North Atlantic Treaty against cyber-attacks. Some Estonian officials invoked Article 5 of the North Atlantic Treaty, but the problem was whether it should also be evaluated under Article 4 of the same Treaty, because, up until the time that the Estonian case occurred, the international community and its organisations had never attempted to apply international law to cyber threats and attacks. NATO applied Article 4 of the Treaty to the Estonian case, and the organisation evaluated cyber threats under Article 4 of the Treaty for the first time in

[1025] "Cyber-attacks on Estonia were the impetus for NATO because they forced the Alliance to change its security trajectory into a more comprehensive approach by extending the development of cyber capabilities also to its members." Laasme, (2012), *op.cit.*, p.9

2008. Moreover, international organisations did not openly define the concept until this case had transpired; thus, neither international organisations nor individual states had any specific policies for solving the problem (e.g. NATO or the state of Turkey). The Estonian case has, thus, become an important turning point in terms of not only better defining the concept of cyber terrorism, but also how international organisations and states should apply international law to acts falling under this category of crime. By establishing new policies and precedents, they will be able to better fight against these types of threat in the future. This decision, the application of Article 4 of the Treaty, however, was not taken in any conscious way, but because NATO did not have any other choice in this regard; they had to adopt that decision in order to ensure the peace and security of the region, as well as that of the international arena as a whole, because as, mentioned earlier, NATO is a peaceful organisation and tries to resolve disputes in peaceful ways. The organisation evaluated the cyber threats under Article 5 of the Treaty in the Wales Summit in 2014, due to the changing nature of the conditions of risks and threats. The decision of the Summit declaration is that for the first time, NATO has evaluated cyber threats under Article 5, collective defence. Also, the Warsaw Summit is important because the organisation has extended the coverage of cyber threats, and hybrid threats can now be evaluated under Article 5 of the North Atlantic Treaty.

The findings of the research is not only demonstrate that threat perceptions, risks and security policies have changed throughout time, but also that whether a threat or a risk is perceived as being a threat or as a risk depends on whether states and international organisations identify them as such. Although many threat perceptions and risks exist in the international arena, whether they are considered as threats or risks thus depends on the official positions of the individual states. As was revealed in this research, a case can be perceived as being a threat or a risk for one state whilst not being similarly perceived by other states in the international community. International organisations, therefore, must identify the cases which are commonly perceived as threats or risks, in order to prevent them from occurring.

When investigating the history of international organisations and the processes they employ to identify threats or risks, one can conclude that there exists no parity between their identifying of the threats and their methods of tackling them, although states and international organisations have tried to apply international law to identify perceived threats. For instance, even though Iran's nuclear weapons are perceived as being a threat by international organisations (such as the UN), Israel’s are not. Thus, the threat perceptions of the UN are based on the political aims of the UN Security Council and, ergo, on the political aims of the USA and other superpowers. These examples are duplicable, but it is important to show how applying Articles 2/4 and 51 of the UN Charter and Article 5 of the North Atlantic Treaty can be problematic if the case is not generally accepted as a risk or threat. As stated above, the Estonian case is a crucial example of the application of Article 5 of the Treaty. Of course, international organisations experienced shock after the collapse of the USSR and had to re-evaluate and accept risks and new threat perceptions after the end of the Cold War in order to survive in the international arena. This problem originates from how international law is applied. Some international laws, such as Article 2/4 of the UN Charter, are not explicit. This sometimes creates problems in terms of how to apply this Article - not to mention Article 51 of the same - to commonly perceived threats.

In Chapter 2, the historical development of the threats perception and risks detailed, and findings showed that nowadays, the risks and threats faced by the international community do not necessarily come directly from states any longer; they also come from rogue states and terrorist organisations. Although counter-terrorism activities usually involve killing people or harming states, the new risks and threats that states are facing do not necessarily include killing or death. The new threats are different from other types of threat, since, with the development of technology, terrorists have been able to use technological tools against the international community for the purposes of creating fear and causing harm. Stealing identities, credit cards, fraud, and other types of cybercrime and cyber terrorism are examples of the new threats which the international community has to face. Moreover, the way in which the international community has tackled these problems clearly reflects the inadequacies of the states and international organisations in identifying and preventing these risks and threats. For example, even though many cyber-attacks have occurred in the international arena against states, many of the states and international organisations which have been affected did not care very much about addressing these problems. Although there was one international agreement which fought cybercrime and cyber problems, it did not provide the expected outcomes, because many states only ratified it years later. For example, even though the Cybercrime Convention was accepted in 2004, Turkey only signed it in 2010, ratifying it four years after its signing.

The second chapter is important in terms of the development of threat perceptions and the changing nature of threats to risks. NATO's first Strategic concept after the Cold War in 1990 was important in changing the focus of the organisation from the concept of threat to risk. With this Strategic Concept, NATO adapted itself to the new era, and this situation can be accepted as NATO becoming a working hypothesis in terms of adapting, changing and continually planning in the face of new circumstances, and the changing policies of cyber security. The acceptation of the application of Articles 4/5 of the North Atlantic Treaty to cyber-attacks shows us this changing and continual planning process.

Also, one of the most significant problems that the international community faces is that of deciding upon a common definition for perceived risks and threats, and this is detailed in the second chapter. Like other problems of the international community, such as terrorism and humanitarian problems, there is no common definition regarding current risks and threat perceptions - particularly the concept of cyber terrorism. By accepting different definitions, the international community cannot share common points regarding these problems. This, in turn, reveals an inextricable situation for the international community. In order to solve this problem, the international community must gather and agree upon the common points shared by threats, and formulate coherent definitions regarding them. If one state only accepts certain aspects of a definition, and other states only accept the other aspects of that same definition, the international community (both states and international organisations) will never be able to solve the problem. Therefore, I believe that if no common definition is provided and agreed upon, the threat itself will grow and cause different problems, thereby making it more difficult to protect the peace and security of the world under international law.

Chapter 3 detailed the application of Game Theory to the thesis. Game Theory was normally used to analyse Cold War term cases, such as the nuclear arms race and the Cuban Missile Crisis, and these cases were also detailed in this chapter to evaluate the application of Game theory to cyber-attacks. Game Theory is a decision-making process, which analyses different strategies in different modes. It also analyses rational behaviour, and when both sides of the cyber-attacks are analysed, we can see that both sides are rational and have strategies. The application of Game Theory to the above cases showed the results of possible strategies. The theory was used to analyse the cyber security policies of NATO and Turkey, and to determine expected payoff when they decided to use any strategy. Also, the Stackelberg security game was used to evaluate the Estonian cyber-attacks, showing the importance of the implementation of mixed strategies during the attacks. The application of Game Theory results showed that Turkey’s cyber security policy could be evaluated under the Zero-Sum game fraction, because Turkey has still only determined their cyber security policies at a lower level, and has not accepted or used other strategies, such as acceptation of cyber terrorism as a threat, nor improved its cyber security policy in accordance with this strategy. Therefore, the application of Zero-Sum game fraction shows us that Turkey has not minimized the maximum possible loss against cyber-terrorists.

Another severe problem is that of applying international law to cyber threats. Like other threat perceptions, there is no common method of applying and implementing international law against cyber threats. For instance, some scholars evaluate cyber threats as armed attacks, whilst others do not. As mentioned above, together with defining the problem, the second phase of solving the problem is that of applying international law appropriately. If the international community's main problem is that of explaining its common problems and threats in different ways (i.e. not having a common definition), then it will become difficult for them to apply international law to those perceived threats. If the international community succeeds in addressing the first phase of the problem, it would be easier to agree on a method of applying international law to such problems. With regards to whether a particular cyber-attack should be considered as an armed attack or not, my opinion is that Schmitt's explanation and Silver's interpretation are the best ways of dealing with this conundrum. If the international community tries to use too many explanations, the problem may become inextricable, and thereby worsened. Silver's interpretation of when cyber-attacks fall under the aegis of international law (i.e. by means of measuring their severity) is a clear way in which the international community can decide which international law can be applied to solving the problem of cyber terrorism.

In addition, if international law clearly explains which situations should be considered as cyber-attacks in the international arena, they could be more successful at absorbing the problems identified by state and international organisational policies, thereby making it easier for the international community to determine whether people/states should be considered as cyber terrorists, and whether those actions constitute acts of war. NATO's cyber security policy is completed, NATO having accepted to evaluate cyber-attacks under Article 5 of the North Atlantic Treaty.

It is not easy to draw a conclusion regarding Turkey's position against cyber threats. Although there have been many instances of cyber threats in the international arena - not to mention many well-designed cyber policies (such as those of Estonia) - Turkey is still trying to form its own cyber security policy. I believe that the policies that are, thus far, in existence cannot guarantee that cyber terrorism activities will be hindered, because its officials have tried to evaluate cyber threats in the narrow sense under the theft, stealing identity and fraud. This, in turn, means that only some problems are eliminated, seeing as only some cases are accepted as being threats or risks; this, however, has not led to the disintegration of cyber terrorism.

To conclude, the international community, including both states and international organisations, should work together in order to solve cyber threats and other problems. This is the only way to ensure the peace and security of the international arena. Although NATO has changed its structure and accepted cyber threats in its agenda, Turkey still lags behind the organisation in terms of the determination of cyber security policies and the application of its cyber legislation. This research suggests that the Estonian case and Estonia’s cyber security policy could become a role model for Turkey to begin building its own new cyber security policy.

7.1. Limitations of the Research

The research had some limitations in certain areas, which have been mentioned separately. For instance, one limitation stemmed from the literature, which does not have any common definition of concepts such as terrorism, cybercrime and cyber terrorism. Therefore, some different definitions of the concepts were given and compared with each other. After that, the researcher gave his own definition to try to solve the international community’s common definition problem.

The second limitation also stemmed from the literature, because the concept of “threat” had not been examined before in detail, and there was also no common definition. The research took the concept of threat from the first nation-states until recent times, and the concept of threat was examined in detail and criticized using different theories. The important shift of NATO with regards to the changing nature of threat to risk was then detailed. Although there were some materials available in the existence, the research applied different theories to evaluate the concept of risk.

Thirdly, academic research is problematic in terms of the application of laws against cyber terrorism. International laws, including the North Atlantic Treaty and the United Nations Charter, were analysed in depth in terms of the use of force and the application of these laws to cyber terrorism, and then various scholars’ and authors’ ideas were used for comparison of their applications. Finally, the researcher highlighted the limitations in the application of international laws to cyber terrorism, and the recommendation was given in Chapter 4 that the international community should adopt Schmitt and Silver’s approach, which argues that cyber-attacks should be considered as armed force only when they are of a severe nature. It may also assist in addressing legal questions about the nature of attack and the method or criteria for determining if it is credible enough on which to base a reasonable decision about whether to act or not to act.

Although there were some limitations, further information was given about the policies, which were criticized in detail. To sum up, I believe that the definition and application of international law will help the international community to solve one of its most pressing problems.

BIBLIOGRAPHY

Books and Articles

Abbott, P., Wallace, C. and Beck, M. (2006), "Chernobyl: Living with Risk and Uncertainty", *Health, Risk& Society*, Vol. 8 (2), Available at: https://www.abdn.ac.uk/socsci/documents/AWB2006.pdf (Accessed at: 15/07/2016)

Akande, D. (2010), "International Organisations" in Evans, M. (ed.) (2010), *International Law*, Oxford: Oxford University Press

Akdeniz, Y. (2009), *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship*, Available at: http://ec.europa.eu/enlargement/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censorship.pdf (Accessed at: 09/11/2013)

Akdoğan, H., Sozer, M. A. and Can, A. (2016), "The Role of NATO and Other International Entities in Counter-Terrorism", in Ekici, S., Akdoğan, H. Ragab, E., Ekici, A. and Warnes, R. (eds.) (2016), *Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations*, Amsterdam: IOS Press

Allison, G. (1969), "Conceptual Models and the Cuban Missile Crisis", *The American Political Science Review*, Vol. 63 (3)

Alpcan, T. and Başar, T. (2005), *A Game Theoretic Analysis of Intrusion Detection in Access Control Systems*, Available at: http://people.virginia.edu/~sdp5f/sys793/presentations/2005/07%20Henry%201012/Papers/alpcan-basar-cdc04_WeA05_6.pdf (Accessed at: 08/09/2016)

Alpcan, T. and Başar, T. (2006), *An Intrusion Detection Game With Limited Observations*, Available at: http://www.tansu.alpcan.org/papers/isdg06.pdf (Accessed at: 08/09/2016)

Alpcan, T. and Başar, T. (2011), *Network Security: A Decision and Game-Theoretic Approach*, Cambridge: Cambridge University Press

Amet, A. K. (2013), "Terrorism and International Law: Cure the Underlying Problem, Not Just the Symptom", *Annual Survey of International&Comparative Law*, Vol. 19 (1), Available at: http://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1168&context=annlsurvey (Accessed at: 18/07/2016)

An, B., Tambe, M., Ordonez, F., Shieh, E. and Kiekintveld, C. (2011), "Refinement of Strong Stackelberg Equilibria in Security Games", *Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence*, Available at: http://teamcore.usc.edu/people/boa/papers/bo-an_aaai11.pdf (Accessed at: 11/06/2016)

An, B., Tambe, M. and Sinha, A. (2015), "Stackelberg Security Games (SSG) Basics and Application Overview", *Nanyang Technological University*, Available at: http://www.ntu.edu.sg/home/boan/papers/Milindchapter.pdf (Accessed at: 12/09/2016)

Anadolu Ajansı (2013), *TSK'da Siber Suçlarla Mücadele Edecek,* Available at: http://www.aa.com.tr/tr/turkiye/239031--tsk-da-siber-suclarla-mucadele-edecek (Accessed at: 13/11/2013)

Angli, M. L. (2013), "What does 'Terrorism' Mean?", in Masferrer, A. and Walker, C. (2013), *Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State,* Cheltenham: Edward Elgar

Anil, S. (2010), "Cyber Security in NATO 2002 to 2020", in Deloitte (2010), "Cyber Security for Government CIO's", *Deloitte 1st European Cyber Security,* Available at: http://www.deloitte.com/assets/Dcom-Namibia/Local%20Assets/Documents/cyber%20security%20round%20table%20report_final.pdf (Accessed at: 05/03/2013)

Annan, K. (2004), "Courage to Fulfil Our Responsibilities", *The Economist,* Available at: http://www.economist.com/node/3445764 (Accessed at: 18/05/2016)

Applegate, S. D. (2009), *Cyber Warfare: Addressing New Threats in the Information Age,* Available at: https://www.academia.edu/1098261/Cyber_Warfare_-_Addressing_New_Threats_in_the_Information_Age (Accessed at: 15/05/2016)

Archick, K. (2006), "Cybercrime: The Council of Europe Convention", *CRS Report for Congress*, Available at: http://www.au.af.mil/au/awc/awcgate/crs/rs21208.pdf (Accessed at: 25/05/2016)

Arend, A. C. and Beck, R. J. (2013), *International Law and The Use of Force,* New York: Routledge

Argomaniz, J. (2010), "The European Union Post 9/11 Counter-Terror Policy Response: An Overview", *Research Institute for European and American Studies,* Research Paper No. 140, Available at: http://www.rieas.gr/images/rieas140.pdf (Accessed at: 05/04/2016)

Arnoldi, J. (2009), *Risk*, Cambridge: Polity Press

Arquilla, J., Ronfeldt, D. and Zanini, M. (1999), "Networks, Netwar and Information-Age Terrorism", in Khalilzad, Z., White, J. P. and Marshall, A. (eds.) (1999), *Strategic Appraisal: The Changing Role of Information in Warfare,* Santa Monica: RAND

Art, R. J. (1996), "Why Western Europe Needs the United States and NATO", *Political Science Quarterly,* Vol. 111(1), Available at: http://www.transatlantic.uj.edu.pl/upload/59_ac3f_Art.WE_Nato.pdf (Accessed at: 13/08/2012)

Associated Press (2005), *Estonia First to Allow Online Voting Nationwide,* Available at: http://www.nbcnews.com/id/9697336/ns/technology_and_science-tech_and_gadgets/t/estonia-first-allow-online-voting-nationwide/#.U2_g0fmSzXs (Accessed at: 10/01/2014)

Associated Press (2007), *Removal of Soviet War Memorial Sparks Deadly Riots in Estonia,* Available at: http://www.foxnews.com/story/2007/04/27/removal-soviet-war-memorial-sparks-deadly-riots-in-estonia/ (Accessed at: 12/04/2014)

Aybet, G. (1999), “NATO’s New Missions”, *Journal of International Relations,* Vol. IV (1), Available at: http://sam.gov.tr/wp-content/uploads/2012/02/GulnurAybet3.pdf (Accessed at: 13/08/2012)

Aybet, G. (2012), “Turkey’s Security Challenges and NATO”, *Carnegie Europe,* Available at: http://carnegieendowment.org/files/Aybet_Brief.pdf (Accessed at: 07/08/2014)

Babu, M., & Parishat, M. (2004). “What is Cybercrime?”, *Computer Crime Research Center,* Available at: http://www.crime-research.org/analytics/702/ (Accessed at: 10/02/2012)

Bahşi, H. and Karabacak, B. (2008), *Ulusal Bilgi Sistemleri Güvenlik Programı,* Available at: http://www.emo.org.tr/ekler/d823125670f66de_ek.pdf (Accessed at: 11/09/2014)

Bakanlar Kurulu Kararı (2013), *2013/5428 SAYILI KARARNAMENİN EKİ,* Available at: http://www.resmigazete.gov.tr/eskiler/2013/10/20131010-1.htm (Accessed at: 20/11/2013)

Bakanlar Kurulu Kararı (2014), *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun,* Available at: http://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm (Accessed at: 20/09/2014)

Bakır, E. (2012), “Türkiye’de Siber Güvenlik”, *Bilim ve Teknik*, Kasım, Available at: http://vizyon21yy.com/documan/genel_konular/bilisim/Turkiyede_Siber_Guvenlik.pdf (Accessed at: 15/09/2014)

Baldwin, D. A. (1995), “Security Studies and the End of the Cold War”, *World Politics*, Vol. 48, Available at:http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1995)%20Security%20Studies%20and%20the%20End%20of%20the%20Cold%20War.pdf (Accessed at: 15/08/2012)

Ballard, J. D., Hornik, J. G. and McKenzie, D. (2002), “Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues”, *American Behavioral Scientist,* Vol: 45(6), Available at: http://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1007&context=scjpeerpubs (Accessed at: 01/04/2015)

Başbakanlık (2012), *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı*, Available at: http://www2.tbmm.gov.tr/d24/1/1-0676.pdf (Accessed at: 20/09/2014)

Başeren, S. H. (2003), *Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmasının Sırları*, Ankara: Ankara Üniversitesi Basımevi

Beck, U. (1992), “From Industrial Society to the Risk Society: Questions of Survival, Social Structure and Ecological Enlightenment”, *Theory, Culture & Society,* Vol. 9 (1)

Beck, U. (1992)*, Risk Society: Towards a New Modernity,* London: SAGE Publications

Beck, U. (1998), Politics of Risk Society, in Franklin, J. (1998), *The Politics of Risk Society,* Cambridge: Polity Press

Beck, U., Bonss, W. And Lau, C. (2003), “The Theory of Reflexive Modernization: Problematic, Hypotheses and Research Programme”, *Theory, Culture&Society,* Vol. 20 (1)

Beck, U. (2006), “Living in the World Risk Society”, *Economy and Society,* Vol. 35 (3), Available at: http://www.skidmore.edu/~rscarce/Soc-Th-Env/Env%20Theory%20PDFs/Beck--WorldRisk.pdf (Accessed at: 22/06/2016)

Beck, U. (2009), *World at Risk*, Cambridge: Polity Press

Becker, S., Seibert, J., Zage, D., Nita-Rotaru, C. and State, R. (2011), *Applying Game Theory to Analyze Attacks and Defenses in Virtual Coordinate Systems*, Available at: http://ds2.cs.purdue.edu/papers/dsn2011_gametheory.pdf (Accessed at: 07/09/2016)

Behnke, A. (2013), *NATO’s Security Discourse After the Cold War: Representing the West,* Oxon: Routledge

Belkin, P., Ek. C., Mages, L. and Mix, D. E. (2009), NATO’s 60th Anniversary Summit, *Congressional Research Service,* Available at: http://www.fas.org/sgp/crs/row/R40454.pdf (Accessed at: 06/05/2013)

Berdal, M. (1999), “International Security After the Cold War: Aspects of Continuity and Change”, in Spillman, K. and Wenger, A. (1999), Towards the 21st Century: Trends in Post-Cold War International Security Policy, *Studies in Contemporary History and Security Policy,* Vol. 4, Available at: http://www.css.ethz.ch/publications/pdfs/Studien_zu_ZS-4.pdf (Accessed at: 14/08/2012)

Bhagyavati, B. (2008), “Social Engineering”, in Janczewski, L. J. and Colarik, A. M. (eds.) (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference

Bıçakçı, S. (2012), “Yeni Savaş ve Siber Güvenlik Arasında NATO’nun Yeniden Doğuşu”, *Uluslararası İlişkiler*, Cilt 9 Sayı 34, Available at: http://www.academia.edu/1828068/The_Rebirth_of_NATO_between_New_War_and_Cyber Security (Accessed at: 13/06/2012)

Bıçakçı, S. (2013), *21. Yüzyılda Siber Güvenlik*, İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Bier, V. M., Cox, L. A. and Azaiez, M. N. (2009), “Why Both Game Theory and Reliability Theory Are Important in Defending Infrastructure Against Intelligent Attacks”, in Bier, V. M. & Azaiez, M. N. (2009), *Game Theoretic Risk Analysis of Security Threats,* New York: Springer

Bilbao, J., Fernandez, J., Jimenez, N., and Lopez, J. (2002), “Voting power in the European Union Enlargement”, *European Journal of Operational Research,* Vol. 143, Available at: http://www.esi2.us.es/~mbilbao/pdffiles/enlargue.pdf (Accessed at: 06/08/2015)

Bilgi Teknolojileri ve İletişim Kurumu (2012), *Cyber Shield Exercise 2012 Final Report,* Available at: http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/dokumanlar/Ek10-cyber_shield_2012_final_report_en.pdf (Accessed at: 15/09/2014)

Biller, J. T. (2012), “Cyber-Terrorism: Finding a Common Starting Point”, *Master Thesis,* Available at: http://media.proquest.com/media/pq/classic/doc/2736442311/fmt/ai/rep/NPDF?_s=WeFenx84aXrPIC9W%2FWolUQH7vfo%3D (Accessed at: 15/12/2014)

Binmore, K. (2007), *Game Theory a Very Short Introduction,* Oxford: Oxford University Press

Bishop, P. (2015), “Cyberterrorism, Criminal Law and Punishment-Based Deterrence”, in Jarvis, L., Macdonald, S. and Chen, T. M. (eds.) (2015), *Terrorism Online: Politics, Law and Technology*, Oxon: Routledge

Blomfield, A. (2007), *Estonia Calls for NATO Cyber-Terrorism Strategy*, Available at: http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html (Accessed at: 15/12/2014)

Borawski, J. and Young, T. D. (2001), *NATO After 2000: The Future of the Euro-Atlantic Alliance*, USA: Praeger Publishers

Bordner, B. (1997), *Rethinking Neorealist Theory: Order Within Anarchy*, Available at: http://www.brucebordner.com/Neorealism.html (Accessed at: 12/08/2012)

Bothe, M. (1967), “Consequences of the Prohibition of the Use of Force: Comments on Arts 49 and 70 of the ILC’s 1966 Draft Articles on the Law of Treaties”, *Heidelberg Journal of International Law*, Available at: http://www.zaoerv.de/27_1967/27_1967_3_c_507_519.pdf (Accessed at: 10/06/2014)

Bowett, D. W. (1958), *Self-Defence in International Law*, Manchester: Manchester University Press

Boyd, C. (2004), “Estonia opens politics to the web*”, BBC*, Available at: http://news.bbc.co.uk/2/hi/technology/3690661.stm (Accessed at: 10/11/2014)

Bozkurt, A. (2010), *Siber Savaş Tatbikatı Ertelendi*, Available at: http://www.bilisimdergisi.org/s127/pdf/8-9.pdf (Accessed at: 12/11/2013)

Brams, S. J. (1985), *Rational Politics: Decisions, Games, and Strategy*, London: Academic Press Limited

Brams, S. J. (1993), “Theory of Moves”, *American Scientist published by Sigma Xi*, Vol. 81, Available at: https://www.acsu.buffalo.edu/~fczagare/Game%20Theory/Theory%20of%20Moves.pdf (Accessed at: 28/07/2016)

Brams, S. J. (2001), Game Theory and the Cuban Missile Crisis, Available at: https://plus.maths.org/content/game-theory-and-cuban-missile-crisis (Accessed at: 04/09/2016)

Brams, S. J. (2003), *Negotiation Games: Applying Game Theory to Bargaining and Arbitration*, London: Routledge

Brandenburger, A. (2007), Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution, Available at: http://www.uib.cat/depart/deeweb/pdi/hdeelbm0/arxius_decisions_and_games/cooperative_game_theory-brandenburger.pdf (Accessed at: 05/09/2016)

Breedlove, P. M. (2015), “Foreword”, in Lasconjarias, G. and Larsen, J. A. (Eds.) (2015), *NATO’s Response to Hybrid Threats*, NDC Forum Paper 24

Broache, A. (2005), *Estonia Pulls off Nationwide Net Voting*, Available at: http://archive.today/20120713045721/http://news.com.com/Estonia+pulls+off+nationwide+Net+voting/2100-1028_3-5898115.html (Accessed at: 10/01/2014)

Brookes, P. (2008), “The Cyber Challenge”, *The Heritage Foundation*, Available at: http://www.heritage.org/research/commentary/2008/03/the-cyber-challenge (Accessed at: 10/11/2014)

Brown, M. E., (ed.) (1996), *Debating the Democratic Peace: An International Security Reader*. Cambridge, MA: The MIT Press

Brown, G., Carlyle, M., Salmeron, J. and Wood, K. (2006), “Defending Critical Infrastructure”, *Interfaces*, Vol. 36 (6), Available at: http://calhoun.nps.edu/bitstream/handle/10945/36732/defending_critical_infrastructure.pdf?sequence=1 (Accessed at: 12/09/2016)

Bryce, T. (2006), “The “Eternal Treaty” from the Hittite Perspective, *BMSAES*, Vol. 6, Available at: http://www.britishmuseum.org/pdf/6a%20The%20Eternal%20Treaty.pdf (Accessed at: 22/08/2012)

Burke, E. (1969), *Reflections on the Revolution in France*, Baltimore: Penguin

Buzan, B. (1983), *People, States and Fear*, Chapel Hill: University of North Carolina Press

Buzan, B. (2000), “Change and Insecurity” Reconsidered”, in Croft, S. And Terriff T. (eds.) (2000), *Critical Reflections on Security and Change*, London: Frank Cass

Carruthers, S. L. (2001), “International History 1900-1945”, in Baylis, J. and Smith, S. (eds.) (2001), *The Globalization of World Politics*, Oxford: Oxford University Press

Carter, D. L. (1995), *Computer Crime: How Techno-Criminals Operate*, Available at: http://www.lectlaw.com/files/cri14.htm (Accessed at: 02/02/2015)

Cavelty, M. D. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Oxon: Routledge

Cavelty, M. D. (2011), “Cyber-Allies: Strengths and Weakness of NATO’s Cyberdefence Posture”, *IP Global Edition*, Vol. 3, Available at: http://www.academia.edu/562910/Cyber-Allies_Strengths_and_weaknesses_of_NATOs_cyberdefense_posture (Accessed at: 13/12/2014)

Chabrow, E. (2014), *NATO Declares Joint Cyber Defence,* Available at: http://www.govinfosecurity.com/nato-declares-joint-cyber-defense-a-7284 (Accessed at: 06/09/2014)

Chailand, G. and Blin, A. (2007), “The Invention of Modern Terror”, in Chailand, G. and Blin, A. (eds.) (2007), *The History of Terrorism*, Berkeley: University of California Press

Chalkiadakis, G., Elkind, E. and Wooldridge, M. (2012), “Cooperative Game Theory: Basic Concepts and Computational Challenges”, *IEE Intelligent Systems*, Available at: http://www.cs.ox.ac.uk/people/michael.wooldridge/pubs/ieeeis2012d.pdf (Accessed at: 05/09/2016)

Charvat, J. (2009), “Cyber Terrorism: A New Dimension in Battlespace”, in Czosseck C. and Geers, K. (eds.) (2009), *The Virtual Battlefield Perspectives on Cyber Warfare*, Amsterdam: IOS Press

Chiarini, G. (2013), *NATO Transformation and Future Challenges*, Available at: http://www.comitatoatlantico.it/en/studi/modern-defense-and-economic-development/ (Accessed at: 10/08/2016)

Chlebik, K. (2010), "Terrorism and Game Theory: From the Terrorists' Point of View", *Pepperdine Policy Review*, Vol. 3, Available at: http://publicpolicy.pepperdine.edu/academics/research/policy-review/2010v3/content/terrorism-and-game-theory.pdf (Accessed at: 03/10/2015)

Christopher F. G. and Griesdorf, M. (2001), "Winners or Losers? Democracies in International Crisis, 1918–94," *American Political Science Review 95*, No. 3 (September 2001)

Cohen, A. (2010), "Cyberterrorism: Are We Legally Ready", *The Journal of Internarional Business and Law*, Available at: https://law.hofstra.edu/pdf/Academics/Journals/JIBL/JIBL_vol9no1_Cohen_Cyberterrorism.pdf (Accessed at: 16/05/2015)

Cohen, A. (2012), "Prosecuting Terrorists at the International Criminal Court: Reevaluating an Unused Legal Tool to Combat Terrorism", *Michigan State International Law Review*, Vol. 20 (2), Available at: http://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1080&context=ilr (Accessed at: 20/06/2016)

Colarik, A. (2006), *Cyber Terrorism Political and Economic Implications*, London: Idea Group Publishing

Colman, A. M. (2003), *Game Theory and Its Applications: In the Social and Biological Sciences*, London: Routledge

Condorelli, L. and Naqvi, Y. (2004), "The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of Date?", in Bianchi, A. (ed.) (2004), *Enforcing International Law Norms Against Terrorism*, Oxford: Hart Publishing

Conrad, P. A. (2002), *Information Warfare: Are You Battlefield Ready?*, Available at: http://www.giac.org/paper/gsec/450/information-warfare-battlefield-ready/101085 (Accessed at: 18/02/2015)

Conte, A. (2010), *Human Rights in the Prevention and Punishment of Terrorism: Commonwealth Approaches: The United Kingdom, Canada, Australia and New Zealand*, Berlin: Springer

Conway, M. (2004), *Cyberterrorism: Media Myth or Clear and Present Danger?*, Available at: http://doras.dcu.ie/505/1/media_myth_2004.pdf (Accessed at: 29/02/2012)

Cooper, R., DeTong, D. V., Forsythe, R. and Ross, T. W. (1989), "Communication in the Battle of the Sexes Game: Some Experimental Results", *The RAND Journal of Economics*, Vol. 20 (4), Available at: http://www.jstor.org/stable/pdf/2555734.pdf (Accessed at: 03/09/2016)

Cooper, R., DeTong, D. V., Forsythe, R. and Ross, T. W. (1993), "Forward Induction in the Battle-of-the-Sexes Games", *The American Economic Review*, Vol. 83 (5), Available at: https://www.jstor.org/stable/pdf/2117562.pdf (Accessed at: 03/09/2016)

Council of Europe (2001), *Convention on Cybercrime*, Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (Accessed at: 15/05/2015)

Council of Europe (2001), *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, Available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=189 (Accessed at: 15/05/2015)

Cox, L. A. (2009), "Game Theory and Risk Analysis, *Risk Analysis*, Vol. 29 (8), Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01247.x/pdf (Accessed at: 10/09/2016)

Cox, M. (2004), "Empire, Imperialism and the Bush Doctrine", *Review of International Studies*, Vol. 30(4), Available at: http://journals.cambridge.org/action/displayAbstract;jsessionid=E3D4DC5045BBA993ECDE33EDC796C7B0.journals?fromPage=online&aid=251273 (Accessed at: 20/08/2012)

Criminal Code (2004), "Law Number 5237", *Number 25611*, Available at: "http://www.wipo.int/wipolex/en/text.jsp?file_i()d=247129 (Accessed at: 10/11/2013)

Croft, A. and Holden, M. (2014), *NATO Backs Spearhead Force to Boost Eastern Defenses*, Available at: http://www.chicagotribune.com/news/sns-rt-us-ukraine-crisis-nato-measures-20140905-story.html#page=1 (Accessed at: 06/09/2014)

Cumper, P. (1999), "Human Rights: History, Development and Classification", in Hegarty, A. and Leonard, S. (eds.) (1999), *A Human Rights: An Agenda for the 21st Century*, London: Cavendish Publishing Limited

Czajka, A. (2011), *The Analysis of the Veto Power in the United Nations Security Council*, Available at: https://www.academia.edu/4028521/The_analysis_of_the_Veto_Power_in_the_United_Nations_Security_Council_Public_International_Law (Accessed at: 15/04/2016)

Czosseck, C., Ottis, R., and Taliharm, A. M. (eds.) (2011), "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security", *International Journal of Cyber Warfare and Terrorism*, Vol. 1(1), Available at: http://www.irma-international.org/viewtitle/61328/ (Accessed at: 03/12/2013)

Çatal, C. (2013), *TSK'dan Siber Savunma Merkezi*, Available at: http://www.hurriyet.com.tr/teknoloji/22405874.asp (Accessed at: 13/11/2013)

Danilovic, V. (2002), *When the Stakes Are High: Deterrence and Conflict Among Major Powers*, USA: University of Michigan Press

Davis, J. W. (2000), *Threats and Promises: The Pursuit of International Influence*, Baltimore, MD: Johns Hopkins University Press

Deighton, A. (2002), "The Eleventh of September and Beyond: NATO", *The Political Quarterly*, Vol. 73 (1), Available at: http://onlinelibrary.wiley.com/doi/10.1111/1467-923X.73.s1.9/abstract, (Accessed at: 10/08/2014)

Denning, D. (2000), *Cyberterrorism*, Available at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Accessed at: 02/03/2012)

Denning, D. E. (2003), *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, H. Comm. on the Armed Services*, Available at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (Accessed at: 07/11/2013)

Department of State, *Strategic Arms Limitation Talks*, Available at: http://www.state.gov/www/global/arms/treaties/salt1.html (Accessed at: 10/08/2012)

Doğrul, M., Aslan, A. and Çelik, E. (2013), "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism", *2011 3rd International Conference on Cyber Conflict*, Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf (Accessed at: 25/07/2016)

Douglas, M. and Wildavsky, A. (1982), *An Essay on the Selection of Technological and Environmental Dangers: Risk and Culture*, Berkeley: University of California Press

Douglas, M. (1992), *Risk and Blame: Essays in Cultural Theory,* London: Routledge

Dowding, K. (2013), "The Prime Ministerialisation of the British Prime Minister", *Parliamentary Affairs,* Vol. 66

Doyle, M. W. (1983), "Kant, Liberal Legacies, and Foreign Affairs, Part 1", *Philosophy & Public Affairs*, Vol 12 (3) (Summer 1983)

Doyle, M. W. (1997), *Ways of War and Peace: Realism, Liberalism, and Socialism*, New York: W. W. Norton

Dülger, M. V. (2005), *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, Available at: http://www.dulger.av.tr/pdf/bilisimsuclariveyctk.pdf (Accessed at: 10/05/2014)

Easley, D. and Kleinberg, J. (2010), *Networks, Crowds, and Markets: Reasoning About A Highly Connected World*, Cambridge: Cambridge University Press

Efthymiopoulos, M. P. (2010), *Challenging NATO's Security Operations in Electronic Warfare: The Policy of Cyber-Defence: the Case of Greece,* Available at: http://www.lse.ac.uk/europeanInstitute/research/hellenicObservatory/pdf/4th_%20Symposium/PAPERS_PPS/FOREIGN_SECURITY_POLICY/EFTHYMIOPOULOS.pdf (Accessed at: 08/04/2012)

Ehala, M. (2009), *The Bronze Soldier: Identity Threat and Maintenance in Estonia*, Available at: http://lepo.it.da.ut.ee/~ehalam/pdf/Identity%20threat.pdf (Accessed at: 12/04/2014)

Elazari, K. (2014), *Hackers: The Internet's Immune System*, Available at: https://www.ted.com/playlists/10/who_are_the_hackers (Accessed at: 12/05/2015)

Ellyatt, H. (2015), *Cyberterrorists to Target Critical Infrastructure*, Available at: http://www.cnbc.com/id/102367777 (Accessed at: 01/04/2015)

Elman, M.F. (ed.) (1997), *Paths to Peace: Is Democracy the Answer?* Cambridge, MA: The MIT Press

Elmas, S. (2013), *Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik,* Ankara: USAK Yayınları

Eloranta, J. (2005), "Why Did The League of Nations Fail", *Sixth European Historical Economics Society Conference*, Available at: http://www.ata.boun.edu.tr/ehes/Istanbul%20Conference%20Papers-%20May%202005/WHY_DID_THE_LEAGUE_OF_NATIONS_FAIL.pdf (Accessed at: 20/05/2016)

Enders, W. and Sandler, T. (1993), "The effectiveness of anti-terrorism policies: A vector autoregression-intervention analysis", *American Political Science Review*, Vol. 87 (4)

Enders, W. and Sandler, T. (1999), "Transnational Terrorism in the Post-Cold War Era", *International Studies Quarterly,* Vol. 43(1)

Enders, W. and Sandler, T. (eds.) (2006), *The Political Economy of Terrorism*, Cambridge: Cambridge University Press

Erol, M. S. and Oğuz, Ş. (2015), "Hybrid Warfare Studies and Russia's Example in Crimea", *Akademik Bakış,* Vol. 9 (17), Available at: http://dergipark.ulakbim.gov.tr/gav/article/viewFile/5000159909/5000144268 (Accessed at: 15/10/2016)

Evans, C. E. (1995), "The Concept of "Threat to Peace" and Humanitarian Concerns: Probing the Limits of Chapter VII of the U.N. Chapter", *Transnational Law & Contemporary Problems*, Vol. 5, Available at: http://heinonline.org/HOL/Page?handle=hein.journals/tlcp5&div=16&start_page=213&collection=journals&set_as_cursor=0&men_tab=srchresults (Accessed at: 05/05/2016)

Evans, G. (2004), *International Law and the United Nations: The Use of Military Force*; Available at: http://www.gevans.org/speeches/speech106.html (Accessed at: 15/01/2015)

Evans, M. (2003), *International Law*, Oxford: Oxford University Press

Ewald, F. (1991), "Insurance and Risk", in Burchell, G. Gordon, C. and Miller, P. (eds.) (1991), *The Foucault Effect: Studies in Governmentality*, London: Harvester

Ewald, F. (1993), "Two Infinities of Risk", in Massumi, B. (1993), *The Politics of Everyday Fear,* Minneapolis: University of Minnesota Press

Fent, T., Feichtinger, G., and Tragler, G. (2002), "A dynamic game of offending and law enforcement", *International Game Theory Review*, Vol. 4(1)

Fidler, D. P., Pregent, R. and Vandurme, A. (2013), "NATO, Cyber Defense, and International Law", *St. John's Journal of International Law&Comparative Law,* Vol. 4(1), Available at: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (Accessed at: 17/05/2016)

Fidler, D. P. (2014), "Overview of International Legal Issues and Cyber Terrorism", *International Law Association*

Finnis, J. (1980), *Natural Law and Natural Rights*, Oxford: Oxford University Press

Flockhart, T. (2016), "Understanding NATO Through Constructivist Theorising", in Webber, M. and Hyde-Price, A. (2016), *Theorising NATO: New Perspectives on the Atlantic Alliance*, London: Routledge

Forester, T. and Morrison, P. (2001), *Computer Ethics*, MIT: MIT Press

Fox, N. (1999), "Postmodern Reflections on 'Risks', 'Hazards' and Life Choices", in Lupton, D. (ed.) (1999), *Risk and Sociocultural Theory*, Cambridge: University of Cambridge Press

Fox, W. T. R. (1959), "The Uses of International Relations Theory", in Fox, W. T. R. (ed.) (1959), *Theoretical Aspects of International Relations*, Notre Dame: University of Notre Dame Press

Fudenberg, D. and Tirole, J. (1991), *Game Theory*, Cambridge, MA: MIT Press

Fuka, J., Obrsalova, I., and Langasek, P. (2012), "Game Theory Application on Terrorism", *Advances in Economics, Risk Management, Political and Law Science*, Available at: http://www.wseas.us/e-library/conferences/2012/Zlin/EPRI/EPRI-37.pdf (Accessed at: 10/09/2016)

Gallis, P. (2003), "NATO's Decision-Making Procedure", *CRS Report for Congress*, Available at: http://fas.org/man/crs/RS21510.pdf (Accessed at: 25/08/2014)

Galvan, M. L. D. L. S. (2011), "Interpretation of Article 39 of the UN Charter (Threat to the Peace) by the Security Council: Is the Security Council a Legislator for the Entire International Community", *Anuario Mexicano de Derecho Internacional*, Vol. XI, Available at: http://www.scielo.org.mx/pdf/amdi/v11/v11a6.pdf (Accessed at: 05/05/2016)

Gasser, H. P. (1986), "Prohibition of terrorist Acts in International Humanitarian Law", *International Review of the Red Cross*, Vol. 26 (253)

Gasser, H.P. (2002), "Acts of Terror "Terrorism" and International Humanitarian Law", *International Review of the Red Cross*, Vol. 84 (847), Available at: https://www.unodc.org/tldb/bibliography/Biblio_Int_humanitarian_law_Gasser_09_2002.pdf (Accessed at: 18/07/2016)

Geers, K. (2011), *Strategic Cyber Security*, Tallinn: CCDCOE Publications

Gervais, M. (2012), "Cyber Attacks and the Laws of War", *Berkeley Journal of International Law*, Vol. 30 (2), Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1422&context=bjil (Accessed at: 15/05/2016)

Ghani, A. and Lockhart, C. (2008), *Fixing Failed States: A Framework For Rebuilding A Fractured World*, Oxford: Oxford University Press

Giddens, A. (1974), *Positivism and Sociology*, Aldershot: Ashgate Publishing Limited

Giddens, A. (1991), *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Stanford: Stanford University Press

Giddens, A. (1998), "Risk Society: The Context of British Politics", in Franklin, J. (ed.) (1998), *The Politics of Risk Society*, Cambridge: Polity Press

Gilmer, C. (2001), *The Future of Information Warfare*, Available at: http://www.sans.org/reading-room/whitepapers/warfare/future-information-warfare-819#__utma=183869984.1510179836.1427206897.1427206897.1427206897.1&__utmb=183869984.4.9.1427206919128&__utmc=183869984&__utmx=&__utmz=183869984.1427206

897.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=-&__utmk=129408012 (Accessed at: 18/02/2015)

Gioia, A. (2006), “The UN Conventions on the Prevention and Suppression of International Terrorism, in Nesi, G. (2006) (ed.), *International Cooperation in Counter-Terrorism: The United Nations and Regional Organisations in the Fight Against Terrorism,* Aldershot: Ashgate Publishing Limited

Golder, B. and Williams, G. (2004), “What is ‘Terrorism’? Problems of Legal Definition”, *UNSW Law Journal*, Vo. 27 (2), Available at: http://www.tamilnation.co/terrorism/terrorism_definition.pdf (Accessed at: 28/04/2016)

Goodman, W. (2010), *Cyber Deterrence: Tougher in Theory than in Practice?,* Available at: http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf (Accessed at: 20/05/2016)

Gooree, J. K. and Holt, C. A. (2000), “Coordination Games”, *Encyclopedia of Cognitive Science*, Available at: http://www.econ.uzh.ch/dam/jcr:ffffffff-d693-da45-0000-00007653d068/CG.pdf (Accessed at: 03/09/2016)

Gordon, M. and Trainor, B. (1995), *The Generals’ War: The Inside Story of the Conflict in the Gulf*, Boston: Little Brown and Co.

Gordon, P. H. (2000), “NATO After 11 September”, *The International Institute for Strategic Studies*, Vol. 43 (4), Available at: http://www.brookings.edu/views/articles/gordon/2002wintersurvival.pdf (Accessed at: 10/08/2014)

Government Resolution (2013), *Finland’s Cyber Security Strategy*, Available at: http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf (Accessed at: 20/02/2015)

Gönül, V. (2010), “Turkey-NATO Relations and NATO’s New Strategic Concept”, *Turkish Policy Quarterly*, Vol. 9 (1), Available at: http://www.turkishpolicy.com/images/stories/2010-01-tpq/15-21.pdf (Accessed at: 07/08/2014)

Görener, A. Ş., (2004), “The Doctrine of Pre-Emption and the War in Iraq under International Law”, *Perceptions*, Available at: http://sam.gov.tr/wp-content/uploads/2012/02/AylinsekerGorener.pdf (Accessed at: 02/10/2015)

Graham, D. E. (2010), “Cyber Threats and the Law of War”, *Journal of National Security Law and Policy*, Vol. 4 (87), Available at: http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf (Accessed at: 13/05/2015)

Gramaglia, M., Tuohy, E. and Pernik, P (2013), “Military Cyber Defence Structures of NATO Members: An Overview”, *Background Paper*, Available at: http://icds.ee/fileadmin/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf (Accessed at: 08/09/2014)

Gratius, S. (2008), “The International Arena and Emerging Powers: Stabilising or Destabilising Forces?”, *FRIDE*, Available at: http://fride.org/descarga/com_emerging_powers_eng_abr08.pdf (Accessed at: 20/12/2015)

Gray, C. (2003), "The Use of Force and The International Legal Order", in Evans, M. (2003), *International Law,* Oxford: Oxford University Press

Gray, C. D. (2008), *International Law and The Use of Force*, Oxford: Oxford University Press

Gray, C. S. (2006), *Another Bloody Century: Future Warfare,* London: Phoenix

Green, J. A. and Grimal, F. (2012), "The Threat of Force as an Action in Self-Defense under International Law", *Vanderbilt Journal of Transnational Law*, Vol. 44, Available at: http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/green-cr.pdf (Accessed at: 06/01/2015)

Grieco J. M. (1988). "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism", *International Organisation,* Vol. 42

Group of Experts Report (2010), *NATO 2020: Assured Security; Dynamic Engagement*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf (Accessed at: 10/04/2012)

Gulick, E. V. (1955), *Europe's Classical Balance of Power,* New York: Norton

Haeni, R. E. (1997), *Information Warfare an Introduction*, Available at: http://www.trinity.edu/rjensen/infowar.pdf (Accessed at: 19/02/2015)

Hafdell, S. (2012), "Turkey-NATO Relations at the 60th Anniversary", *Policy Update*, No: 2, Available at: http://www.gpotcenter.org/dosyalar/PU2_NATO_Hafdell_MAR2012.pdf (Accessed at: 07/08/2014)

Hall, R. A. (2000), "Theories of Collective Action and Revolution: Evidence from the Romanian Transition of December 1989", *Europe-Asia Studies*, Vol. 52 (6)

Hallion, R. P. (1997), *Storm Over Iraq: Air Power and the Gulf War,* Washington: Smithsonian Books

Hamilton, S. N., Miller, W. L., Ott, A. and Saydjari, O. S. (2002), "The Role of Game Theory in Information Warfare", *Proceedings of the 4th Information Survivability Workshop,* Available at: https://verify.iaik.tugraz.at/research/pub/Ausgewaehltekapitel/WebHome2009/GT_in_IW.pdf (Accessed at: 10/09/2016)

Hansen, L. and Nissenbaum, H. (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly,* Vol. 53, Available at: https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf (Accessed at: 18/05/2016)

Hardy, K. and Williams, G. (2014), "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism", in Chen, T. M., Jarvis, L. and Macdonald, S. (2007), *Cyberterrorism: Understanding Assessment, and Response,* London: Springer

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlani A., Perdue, W., Spiegel, J. (2012), "The Law of Cyber-Attack", *California Law Review*, Available at:

http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf (Accessed at: 05/05/2015)

Haubler, U. (2010), *Cyber Security and Defence From The Perspective of the Articles 4 and 5 of the NATO Treaty*, Available at: http://www.ccdcoe.org/publications/legalproceedings/Haussler_CDfromArticles4and5Perspective.pdf (Accessed at: 10/08/2014)

Hawks, B. B. (2011), *Cyber Terror: The Borderless Danger*, Available at: http://www.inter-disciplinary.net/wp-content/uploads/2011/05/banuhawksepaper.pdf (Accessed at: 11/04/2012)

Heads of State and Government (1999), *The Alliance's Strategic Concept,* Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Accessed at: 19/08/2016)

Heads of State and Government (2006), *Comprehensive Political Guidance*, Available at: http://www.nato.int/cps/en/natolive/official_texts_56425.htm (Accessed at: 23/08/2012)

Heads of State and Government (2010), *Active Engagement, Modern Defence*, Available at: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (Accessed at: 24/08/2012)

Healey, J. and Bochoven, L.V. (2012), "NATO‘s Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council Issue*, February 2012

Heng, Y. K. (2006), *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, London: Routledge

Heng, Y. K. (2006), "The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society", *International Relations*, Vol. 20 (1), Available at: http://ire.sagepub.com/content/20/1/69.full.pdf+html?hwshib2=authn%3A1472486035%3A20160828%253Aac9c830f-b0c0-4084-9f42-11b0f3c242a4%3A0%3A0%3A0%3AePN6ZQXBeRR1k%2FrdPv5wMA%3D%3D (Accessed at: 23/06/2016)

Herz, J. H. (1950), "Idealist Internationalism and the Security Dilemma", *World Politics*, Vol. 2 (2)

Herzog, S. (2011), "Revisiting the Estonian Cyber-Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Vol. 2(4), Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss (Accessed at: 20/05/2016)

Hey, J. A. K. (ed.) (2003), *Small States in World Politics: Explaining Foreign Policy Behavior,* London: Lynne Rienner Publishers

Hobbes, T. (1651) *Leviathan,* London, Available at: http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/hobbes/Leviathan.pdf (Accessed at: 10/05/2012)

Hoffman, P. (2004), "Human Rights and Terrorism", *Human Rights Quarterly,* Vol. 26 (4), Available at: https://muse.jhu.edu/article/174729/pdf (Accessed at: 18/07/2016)

Hoffman, F. G. (2007), *Conflict in the 21st Century: The Rise of Hybrid War,* Arlington: Potomac Institute for Policy Studies

Hughes, R. B. (2008), “NATO and Global Cyber Defence”, in Shepherd, R. (2008), *The Bucharest Conference Papers*, London: Chatham House

Hughes, R. B. (2009), *NATO and Cyber Defence: Mission Accomplished,* Available at: http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf (Accessed at: 05/07/2012)

Huhtinen, A. M. (2007), “Different Types of Information Warfare”, in Anttiroiko, A. V. and Malkia, M. (2007), *Encyclopedia of Digital Government*, London: Idea Group Reference

Human Rights Council (2010), *Counter-Terrorism and the Protection of Human Rights,* Available at: http://www.humanrightsadvocates.org/wp-content/uploads/2010/05/HRC13_Counter-terrorism_and_Human-Rights.pdf (Accessed at: 19/07/2016)

Hunker, J. (2010), “Cyber War and Cyber Power: Issues for NATO Doctrine”, *NATO Defence College,* No 62, Available at: http://www.ndc.nato.int/research/series.php?icode=1 (Accessed at: 08/03/2012)

Hunker, J. (2013), “NATO and Cyber Security”, in Herd, G. P. and Kriendler, J. (eds.) (2013), *Understanding NATO in the 21st Century,* Oxon: Routledge

Iasiello, E. (2013), “Cyber Attack: A Dull Tool to Shape Foreign Policy”, *5th International Conference on Cyber Conflict*, Available at: https://ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf (Accessed at: 17/05/2016)

Ibidunmoye, E. O., Alese, B. K. and Ogundele, O. S. (2013), “Modelling Attacker-Defender Interaction as a Zero-Sum Stochastic Game”, *Journal of Computer Sciences and Applications*, Vol. 1(2), Available at: http://pubs.sciepub.com/jcsa/1/2/3/ (Accessed at: 10/09/2016)

ICC Turkey (2011), *Promoting and Protecting Intellectual Property in Turkey,* Available at: http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/International-engagement-and-Advocacy/Country-Initiatives/Turkey/ (Accessed at: 15/07/2016)

Ikuenobe, P. (2003), “Optimising Reasonableness, Critical Thinking and Cyberspace”, *Education Philosophy and Theory*, Vol. 35 (4)

Information and Communication Technologies Authority of Turkey and TUBITAK (2011), *National Cyber Security Exercise 2011 Final Report*, Available at: http://www.uekae.tubitak.gov.tr/uekae_content_files/siber_tatbikat_raporlari/USGT_2011_en.pdf (Accessed at: 12/11/2013)

International Court of Justice (1984), *Application Instituting Proceedings filed the Registry of the Court on 9 April 1984: Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, Available at: http://www.icj-cij.org/docket/files/70/9615.pdf (Accessed at: 30/08/2015)

International Court of Justice (1986), *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America),* Available at: http://www.icj-cij.org/docket/files/70/6503.pdf (Accessed at: 15/01/2015)

Irshaid, F. (2014), *How ISIS is Spreading Its Message Online,* Available at: http://www.bbc.com/news/world-middle-east-27912569 (Accessed at: 08/05/2015)

Isa, F. G. (2006), “International Protection of Human Rights”, in Isa, F. G. and F. K. D. (eds.) (2006), *International Protection of Human Rights: Achievements and Challenges*, Available at: https://doc.es.amnesty.org/cgi-bin/ai/BRSCGI/International%20Protection%20of%20Human%20Rights:%20Achievements%20and%20Challenges?CMD=VEROBJ&MLKOB=25926890808 (Accessed at: 21/05/2016)

İstanbul Ticaret Odası (2011), Bilişim Teknolojileri ve e-Ticaret Şubesi, *Bilişim ve e-Ticaret Bülteni*, Şubat, Available at: http://www.ito.org.tr/itoyayin/SY059208.pdf (Accessed at: 15/09/2014)

Jain, M., Kardeş, E. and Ordonez, F. (2010), “Security Games with Arbitrary Schedules: A Branch and Price Approach”, *Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence*, Available at: http://teamcore.usc.edu/manish/files/aaai10.pdf (Accessed at: 11/06/2016)

Jain, M., An, B. and Tambe, M. (2013), “Security Games Applied to Real-World: Research Contributions and Challenges”, in Jajodia, S., Ghosh, A. K., Subrahmanian, V. S., Swarup, V., Wang, C. and Wang, X. S. (2013), *Moving Target Defense II: Application of Game Theory and Adversarial Modelling*, London: Springer

Jalil, S. A. (2003), “Countering Cyber Terrorism Effectively: Are We Ready To Rumble?”, *SANS Institute*, Available at: http://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (Accessed at: 01/04/2015)

Janczewski, L. J. and Colarik, A. M. (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference

Jarvis, L., Nouri, L. and Whiting, A. (2014), “Understanding, Locating and Constructing Cyberterrorism”, in Chen, T. M., Jarvis, L. and Macdonald, S. (eds.) (2014), *Cyberterrorism: Understanding, Assessment, and Response*, London: Springer

Javidi, M. M. and Aliahmadipour, L. (2015), “Game Theory approaches in Taxonomy of Intrusion Detection for MANETs”, *Computer Engineering and Applications*, Vol. 4 (1)

Joubert, V. (2012), “Five Year’s After Estonia’s Cyber-Attacks: Lessons Learned for NATO?”, *Research Paper*, Available at: http://www.ndc.nato.int/news/news.php?icode=394 (Accessed at: 01/05/2016)

Kalafat, H. (2011), *Yeni Bir Tip Savaş: Siber Saldırı ve Anonymous Örneği*, Available at: http://yenimedya.wordpress.com/2011/06/15/yeni-bir-tip-savas-siber-saldiri-ve-anonymous-ornegi/ (Accessed at: 10/11/2013)

Kaminski, R. T. (2010), “Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions”, *Conference on Cyber Conflict Proceedings 2010*, Estonia

Kant, I. (1795), *Perpetual Peace: A Philosophical Sketch*, Available at: http://www.constitution.org/kant/perpeace.htm#04 (Accessed at: 23/07/2012)

Kaplan, E. (2009), Terrorists and the Internet, *Council on Foreign Relations*, Available at: http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p1 (Accessed at: 08/05/2015)

Kaplan, L. (2007), *NATO 1948: The Birth of the Transatlantic Alliance*, Plymouth: Rowman&Littlefield Publishers

Karabacak, B. (2010), *İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları*, Available at: https://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html (Accessed at: 16/09/2014)

Kaska, K., Taliharm, A. and Tikk, E. (eds.) (2011), "Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007", *Cooperative Cyber Defence Centre of Excellence*, Tallinn: Estonia

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X., and Ratick, S. (1988), "The Social Amplification of Risk: A Conceptual Framework", *Risk Analysis*, Vol. 8 (2)

Kasperson, R. E. and Kasperson, J. X. (2005), "Considerations and Principles for Risk Communication for Industrial Accidents", in Kasperson, R. E. and Kasperson, J. X. (eds.) (2005), *The Social Contours of Risk: Publics, Risk Communication and The Social Amplification of Risk*, London: Earthscan

Kasperson, J. X. and Kasperson, R. E. (eds.) (2005), *The Social Contours of Risk Volume 2: Risk Analysis, Corporations & the Globalization of Risk*, London: Earthscan

Kassimeris, G. & Buckley, J. (2010), *The Ashgate Research Companion to Modern Warfare*, Farnham: Ashgate Publishing Limited

Keegan, J. (2000), *The First World War*, the UK: Vintage

Kelsen, H. (2000), *The Law of the United Nations: A Critical Analysis of Its Fundamental Problems*, New Jersey: The Lawbook Exchange

Kemos, A. (2015), *The Influence of Thucydides in the Modern World*, Available at: http://www.hri.org/por/thucydides.html (Accessed at: 03/01/2016)

Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordonez, F. and Tambe, M. (2009), "Computing Optimal Randomized Resource Allocations for Massive Security Games", *8th International Conference on Autonomous Agents and Multiagent Systems*, Available at: http://delivery.acm.org/10.1145/1560000/1558108/p689-kiekintveld.pdf?ip=85.99.163.111&id=1558108&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2EA13CBF7F1C3C7DF4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=678714832&CFTOKEN=92564710&__acm__=1475925958_4cdcf7992682e234cfbb37f986c7af1d (Accessed at: 11/06/2016)

King, L., *Eannatum of Lagash 2454-2455 BC*, Available at: http://www.cristoraul.com/ENGLISH/readinghall/GalleryofHistory/Ancient-People/EANNATUM.html (Accessed at: 22/08/2012)

Kleimann, D. (2006), "Positivism, the New Haven School, and the Use of Force in International Law", *Brussels Journal of International Studies*, Vol. 3, Available at: https://www.kent.ac.uk/brussels/documents/journal/2006/David%20Kleimann%20-%20Positivism%20the%20New%20Haven%20School%20and%20the (Accessed at: 03/12/2015)

Klimburg, A. (ed.) (2012), *National Cyber Security Framework Manual,* Tallinn: NATO CCDCOE Publications, Available at: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Accessed at: 05/09/2013)

Kolokoltsov, V. N. and Malafayev, O. A. (2010), *Understanding Game Theory: Introduction to the Analysis of Many Agent Systems with Competition and Cooperation*, London: World Scientific

Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., and Tambe, M. (2011), "Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness", *Journal of Artificial Intelligence Research*, Vol. 41, Available at: http://www.aaai.org/Papers/JAIR/Vol41/JAIR4109.pdf (Accessed at: 11/06/2016)

Kostyuk, N. (2013), "The Digital Prisoner's Dilemma: Challenges and Opportunities for Cooperation", *World Cyberspace Cooperation Summit IV*, Available at: http://cybersummit.info/sites/cybersummit.info/files/The%20Digital%20Prisoner's%20Dilemma-Challenges%20and%20Opportunities%20for%20Cooperation_Nadiya%20Kostyuk%20.pdf (Accessed at: 12/09/2016)

Koufa, K. (2002), "Human Rights and Terrorism in the United Nations", in Alfredsson, G. and Stravropoulou (eds.) (2002), *Justice Pending: Indigenous Peoples and Other Good Causes*, The Hague: Martinus Nijhoff Publishers

Krahmann, E. (2005), "From State to Non-State Actors: The Emerge Of Security Governance", in Krahmann, E. (ed.) (2005), New *Threats and New Actors in International Security*, New York: Palgrave Macmillan

Kramer, S. N. (1963), *The Sumerians; Their History, Culture and Character,* Chicago: University of Chicago Press

Kull, S., Ramsay, C. and Lewis, E. (2003), "Misperceptions, The Media and the Iraq War", *Political Science Quarterly,* Vol .118(4), Available at: http://www.jstor.org/discover/10.2307/30035697?uid=3738032&uid=2&uid=4&sid=21101481037753 (Accessed at: 21/08/2012)

Laasme, H. (2012), "The Role of Estonia in Developing NATO's Cyber Strategy", *Cicero Foundation Great Debate Paper,* No: 12/8, Available at: http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf (Accessed at: 02/10/2015)

Lachow, I. (2009), "Cyber Terrorism: Menace or Myth?", in Kramer, F. D., Starr, S. H. and Wentz, L. K. (2009), *Cyberpower and National Security*, Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-19.pdf (Accessed at: 08/05/2015)

LaFeber, W. (2002), "The Bush Doctrine", *Diplomatic History*, Vol. 26 (4), Available at: http://onlinelibrary.wiley.com/doi/10.1111/1467-7709.00326/abstract (Accessed at: 20/08/2012)

Lagazio, M. (2016), "A Taxonomy of Cybercrime in the Financial Sector: A Comprehensive Approach to Countermeasures", in Taplin, R. (2016), *Managing Cyber Risk in the Financial Sector: Lessons From Asia, Europe and the USA*, New York: Routledge

Lapan, H. E. and Sandler, T. (1993), “Terrorism and Signalling”, *European Journal of Political Economy*, Vol. 9, Available at: http://ac.els-cdn.com/017626809390006G/1-s2.0-017626809390006G-main.pdf?_tid=f8e4c702-8356-11e6-ba11-00000aacb361&acdnat=1474832204_197185a5e5e72c040eaab65155a4fd40 (Accessed at: 10/09/2016)

Larrain, J. (1979), *The Concept of Ideology,* London: Hutchinson Education

Laquer, W. (2001), *A History of Terrorism*, New Jersey: Transaction Publishers

Lash, S. (2003), “Reflexivity as Non-Linearity”, *Theory, Culture&Society,* Vol. 20 (2)

Law, R. (2009), *Terrorism A History,* Cambridge: Polity Press

Lawson, S. M. (2002), *Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure*, Available at: http://www.sans.org/reading-room/whitepapers/warfare/information-warfare-analysis-threat-cyberterrorism-critical-infrastruc-821#__utma=183869984.1510179836.1427206897.1427206897.1427206917.2&__utmb=183869984.1.9.1427223458399&__utmc=183869984&__utmx=-&__utmz=183869984.1427206897.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=-&__utmk=175029154 (Accessed at: 12/05/2015)

Lee, D. R. (1988), “Free Riding and Paid Riding in the Fight Against Terrorism”, *The American Economic Review*, Vol. 78 (2), Available at: https://www.jstor.org/stable/pdf/1818091.pdf (Accessed at: 10/09/2016)

Lee, M. (2006), *How Do Small States Affect the Future Development of the E.U.*, New York: Nova Science Publishers

Lehti, M., Jutila, M., and Jokisipila, M. (2009), “Never Ending Second World War: Public Performances of National Dignity and Drama of the Bronze Soldier”, *Journal of Baltic Studies* 39(4): Available at: http://blogs.helsinki.fi/majutila/files/2009/07/nesww.pdf (Accessed at: 12/04/2014)

Lewis, B. (2004), *The Crisis of Islam*, London: Phoenix Paperback

Lewis, J. A. (2002), “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats”, *CSIS,* Available at: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (Accessed at: 11/03/2015)

Liang, X. and Xiao, Y. (2013), “Game Theory for Network Security”, *IEEE Communications Surveys&Tutorials*, Vol. 15 (1), Available at: http://yangxiao.cs.ua.edu/IEEE_COMST_game_2013.pdf (Accessed at: 07/09/2016)

Libicki, M. C. (1995), *What is Information Warfare?,* The Centre for Advanced Concepts and Technology

Libicki, M. (2007), *Conquest in Cyber Space: National Security and Information Warfare,* Cambridge: Cambridge University Press

Lidskog, R., and Sundqvist, G. (2013), “Sociology of Risk”, in Roeser, S., Hillerbrand, R., Sandin, P., and Peterson, M. (eds.) (2013), *Essentials of Risk Theory*, London: Springer

Liebe, L. A. (2002), NATO’s New Strategic Concept: Implications for a Transforming Army, *School of Advanced Military Studies*

Locke, J. (1690), *Second Treatise of Government,* Edited with an Introduction by Macpherson, C. B. (1980), Indiana: Hackett Publishing Company

Lorca, A. B. (2014), *Mestizo International Law: A Global Intellectual History 1842-1933*, Cambridge: Cambridge University Press

Lowe, J. (1990), *The Concert of Europe: International Relations 1814-70*, London: Hodder Arnold

Luhmann, N. (1989), *Ecological Communication*, Translated by Bednarz, J. (1989), Chicago: The University of Chicago Press

Luhmann, N. (1994), *Social Systems*, Translated by Bednarz, J. and Baecker, D. (1995), Stanford: Stanford University Press

Lupton, D. (2013), *Risk,* Oxon: Routledge

Lye, K.W. and Wing, J. M. (2005), “Game Strategies in Network Security”, *International Journal of Information Security,* Available at: http://www.cs.cmu.edu/~wing/publications/LyeWing05.pdf (Accessed at: 07/09/2016)

Lyman, M. and Potter, G. (1998), *Organized Crime*, New Jersey: Prenhall

Macdonald, S. and Jarvis, L. (2014), “What is Cyberterrorism? Findings From a Survey of Researchers”, *Terrorism and Political Violence,* Vol. 27 (4), Available at: http://www.tandfonline.com/doi/full/10.1080/09546553.2013.847827 (Accessed at: 22/07/2016)

Machiavelli, N. (1952), *The Prince,* Oxford: Oxford University Press

Mackuen, M., Erikson R. and Stimson, J. (1992), “Peasants or Bankers? The American Electorate and the U.S. Economy”, *American Journal of Political Science,* Vol. 86 (3)

Mahmood, F. (2013), “Power Versus the Sovereign Equality of States: The Veto, the P-5 and United Nations Security Council Reforms”, *Perceptions,* Volume XVIII (4), Available at: http://sam.gov.tr/wp-content/uploads/2014/03/Fakiha_Mahmood.pdf (Accessed at: 15/04/2016)

Malksoo, M. (2007), *The Fallen ‘Bronze Soldier’ … (A Response to: Is This the Order we wanted?),* Available at: http://www.icds.ee/index.php?id=73&tx_ttnews%5Btt_news%5D=164&tx_ttnews%5BbackPid%5D=99&cHash=bcff323714 (Accessed at: 12/04/2014)

Manshaei, M. H., Zhu, Q., Alpcan, T., Başar, T., and Hubaux, J. P. (2010), “Game Theory Meets Network Security and Privacy”, *EPFL Technical Report,* Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.187.9377&rep=rep1&type=pdf (Accessed at: 07/09/2016)

Marfleet, B. G. (2000), "The Operational Code of John F. Kennedy during the Cuban Missile Crisis: A Comparison of Public and Private Rhetoric", *Political Psychology,* Vol. 21 (3)

Marion, N. E. (2010), “The Council of Europe’s Cyber Crime Treaty: An Exercise in Symbolic Legislation”, *International Journal of Cyber Criminology,* Vol. 4 (1&2), Available at: http://www.cybercrimejournal.com/marion2010ijcc.pdf (Accessed at: 25/05/2016)

Marks, S. (2006), “International Law and the ‘War on Terrorism’: Post 9/11 Responses by the United States and Asia Pacific Countries”, *Asia Pacific Law Review*, Vol. 14 (1), Available at: https://cdn1.sph.harvard.edu/wp-content/uploads/sites/580/2012/09/spm_Terrorism_and_IL_APLR_2006_vol14.pdf (Accessed at: 21/05/2016)

Markwell, D. (2006), *John Maynard Keynes and International Relations*, Oxford: Oxford University Press

Martinelli, A. (2005), *Global Modernization: Rethinking the Project of Modernity*, London: SAGE Publications

Mastny, V. and Byrne, M. (2006), *A Cardboard Castle?: An Inside History of the Warsaw Pact, 1955-1991,* New York: Central University Press

Matusitz, J. (2009), “A Postmodern Theory of Cyberterrorism: Game Theory”, *Information Security Journal: A Global Perspective*, Vol. 18 (6), Available at: http://www.tandfonline.com/doi/pdf/10.1080/19393550903200474?needAccess=true (Accessed at: 01/07/2016)

Maza, C. (2016), “Did Ukraine’s Cyberattacks Originate in Russia?”, *Atlantic Council*, Available at: http://www.atlanticcouncil.org/blogs/new-atlanticist/did-ukraine-s-cyberattacks-originate-in-russia (Accessed at: 15/10/2016)

McAdams, R. H. (2009), “Beyond the Prisoners’ Dilemma: Coordination, Game Theory, and the Law”, *Southern Law Review,* Vol. 82 (209), Available at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2648&context=journal_articles (Accessed at: 03/09/2016)

Mcconnell International (2000), “Cybercrime...and Punishment*?” Archaic Laws Threaten Global Information*, Available at: http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf (Accessed at: 14/11/2013)

McDougal, M. S. and Reisman, W. M. (1968), “Rhodesia and the United Nations: The Lawfulness of International Concern”, *The American Journal of International Law,* Vol. 62, Available at: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1663&context=fss_papers (Accessed at: 05/05/2016)

Mcgee, J. (2011), “NATO and Cyber Defense: A Brief Overview and Recent Events’ exercises”, *Centre for Strategic and International Studies*, Available at: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events (Accessed at: 03/09/2014)

McGoldrick, D. (2004), *From “9-11” to the “Iraq War 2003”: International Law in a Age of Complexity,* Portland: Hart Publishing

McMahon, R. J. and Zeiler, T. W. (Eds.) (2012), *U.S. Foreign Policy: A Diplomatic History*, London: CQ Press

McNulty, D. (2015), *The Basics of Game Theory*, Available at: http://www.investopedia.com/articles/financial-theory/08/game-theory-basics.asp (Accessed at: 10/12/2015)

McSweeney, B. (1999), *Security, Identity and Interests: A Sociology of International Relations*, Cambridge: Cambridge University Press

Mehlmann, A. (2000), *The game's afoot! Game Theory in myth and paradox*, Providence, RI: American Mathematical Society

Merriam, M. J. J. (2010), "Natural Law and Self-Defense", *Military Law Review*, Vol. 206, Available at:http://poseidon01.ssrn.com/delivery.php?ID=253020073123121008114081107025012028059064002079017045002024010027112068127012004078097103011016022127108107074127089123116127117039004050076082105100096078106084090068005079103118082085112004002094070080107123098109109007019101091095027113118083081003&EXT=pdf (Accessed at: 03/12/2015)

Military Committee (1957), *M.C. 14/2 Overall Strategic Concept for the Defense of The North Atlantic Treaty Organisation Area*, Available at: http://www.nato.int/docu/stratdoc/eng/a570523a.pdf (Accessed at: 06/08/2012)

Military Committee (1957), *Measures to Implement the Strategic Concept,* Available at: http://www.nato.int/docu/stratdoc/eng/a570523b.pdf (Accessed at: 07/08/2012)

Military Committee (1968), *M.C. 14/3 Overall Strategic Concept for the Defense of The North Atlantic Treaty Organisation Area,* Available at: http://www.nato.int/docu/stratdoc/eng/a680116a.pdf (Accessed at: 07/08/2012)

Mill, J. S. (2003), *Auguste Comte and Positivism*, London: Kessinger Publishing

Ministry of Defence (2008), *Cyber Security Strategy*, Available at: http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (Accessed at: 12/01/2015)

Ministry of Economic Affairs and Communication (2014), *2014-2017 Cyber Security Strategy*, Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf (Accessed at: 12/01/2015)

Mises, R. V. (1951), *Positivism; A Study in Human Understanding*, Cambridge: Harvard University Press

Mishra, A. and Mishra, D. (2008), "Cyber Stalking: A Challenge for Web Security", in Janczewski, L. J. and Colarik, A. M. (eds.) (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference

Mishra, R. C. (2004), *Terrorism Implications of Tactics and Technology*, Delhi: Authorspress

Moore, R. R. (2007), *NATO's New Mission: Projecting Stability in a Post-Cold War* World, London: Praeger Security International

Moseley, A. (2015), “Political Realism”, *Internet Encyclopedia of Philosophy,* Available at: http://www.iep.utm.edu/polreal/ (Accessed at: 03/01/2016)

Murphy, S. D. (1996), *Humanitarian Intervention: The United Nations in an Evolving World Order,* Philadelphia: University of Pennsylvania Press

Murphy, S. (2005), “The Doctrine of Pre-emptive Self-Defence”, *Villanova Law Review*, Vol. 699, Available at: http://lsgs.georgetown.edu/programs/nlp/preventivewar/Villanova%20Preemption%20Article%20Final.pdf (Accessed at: 05/10/2013)

Muti, A., Tajer, K. and Macfaul, L. (2014), “Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions”, *Remote Control Project*, Available at: http://remotecontrolproject.org/wp-content/uploads/2014/10/Vertic-Report.pdf (Accessed at: 08/05/2013)

Myerson, R. (2001), *Game Theory Analysis of Conflict*, Cambridge: Harvard University Press

Mythen, G. (2004), *Ulrich Beck: A Critical Introduction to the Risk Society*, London: Pluto Press

Nash, J. (1950), “Equilibrium Points in N-Person Games”, *Proceedings of the National Academy of the USA”*, Vol. 36(1)

National Security Council (2002), *The National Security Strategy of the United States*, Available at: http://www.whitehouse.gov/nsc/nssall.html (Accessed at: 20/08/2012)

NATO (1990), *London Declaration on a Transformed North Atlantic Alliance*, Available at: http://www.nato.int/docu/comm/49-95/c900706a.htm (Accessed at: 15/08/2012)

NATO (1991), *The Alliance’s New Strategic Concept*, 7 November, Available at: http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Accessed at: 10/04/2014)

NATO (1999), *Statement by the North Atlantic Council on Kosovo*, 30 January, Available at: http://www.nato.int/docu/pr/1999/p99-012e.htm (Accessed at: 25/09/2013)

NATO (1999), *The Alliance’s Strategic Concept*, 24 April, Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Accessed at: 15/04/2012)

NATO (2002), *Prague Summit Declaration*, Available at: http://www.nato.int/docu/pr/2002/p02-127e.htm (Accessed at: 01/06/2012)

NATO (2005), *NATO and the Scourge of Terrorism: What is Article 5?*, Available at: http://www.nato.int/terrorism/five.htm (Accessed at: 14/01/2015)

NATO (2006), *Riga Summit Declaration*, Available at: http://www.nato.int/docu/pr/2006/p06-150e.htm (Accessed at: 04/05/2012)

NATO (2006), *Comprehensive Political Guidance*, Available at: http://www.nato.int/cps/en/natolive/official_texts_56425.htm (Accessed at: 12/10/2016)

NATO (2006), *Handbook*, Available at: http://www.nato.int/docu/handbook/2006/hb-en-2006.pdf (Accessed at: 17/08/2016)

NATO (2008), *Bucharest Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_8443.htm (Accessed at: 02/01/2012)

NATO (2009), *Strasbourg/Kehl Summit Declaration*, Availablet at: http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease (Accessed at: 21/07/2013)

NATO (2010), *NATO's New Strategic Concept: Group of Experts*, Available at: http://www.nato.int/strategic-concept/experts-strategic-concept.html (Accessed at: 20/04/2013)

NATO (2010), "Active Engagement, Modern Defence", *Strategic Concept*, Available at: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (Accessed at: 04/06/2013)

NATO (2010), *Lisbon Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease (Accessed at: 04/06/2013)

NATO (2010), *NATO 2020: Assured Security; Dynamic Engagement*, Available at: http://www.nato.int/cps/en/natolive/official_texts_63654.htm#p2 (Accessed at: 24/08/2012)

NATO (2011), *Bilgilendirme*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf (Accessed at: 08/05/2013)

NATO (2011), *Defending the Networks: The NATO Policy on Cyber Defence*, Available at: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (Accessed at: 04/09/2013)

NATO (2012), *NATO Rapid Reactions Team to Fight Cyber Attack*, Available at: http://www.nato.int/cps/en/natolive/news_85161.htm (Accessed at: 08/07/2014)

NATO (2012), "Tackling New Security Challenges", *Briefing*, Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120116_new-security-challenges-e.pdf (Accessed at: 16/09/2014)

NATO (2012), *Chicago Summit Declaration*, Available at: http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease (Accessed at: 06/10/2013)

NATO (2014), *A Short History of NATO*, Available at: http://www.nato.int/history/nato-history.html (Accessed at: 04/09/2014)

NATO (2014), *Collective Defence*, Available at: http://www.nato.int/cps/en/natohq/topics_110496.htm? (Accessed at: 04/09/2014)

NATO (2014), *The NATO Defence Planning Process*, Available at: http://www.nato.int/cps/en/natolive/topics_49202.htm (Accessed at: 15/08/2014)

NATO (2014), *Wales Summit Declaration*, Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (Accessed at: 06/09/2014)

NATO (2015), *Press Statements*, Available at: http://www.nato.int/cps/en/natohq/opinions_125361.htm (Accessed at: 14/10/2016)

NATO (2015), *Turkey: NATO, EU and its evolving foreign and security policy*, Available at: http://natolibguides.info/Turkey (Accessed at: 15/05/2016)

NATO (2016), *Warsaw Summit Communique*, Available at: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed at: 13/10/2016)

NATO (2016), *Cyber Defence*, Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed at: 12/10/2016)

NATO Cooperative Cyber Defence Centre of Excellence (2010), *Baltic Cyber Shield 2010*, Available at: http://www.ccdcoe.org/baltic-cyber-shield-2010.html (Accessed at: 11/08/2014)

NATO Cooperative Cyber Defence Centre of Excellence (2012), *Locked Shields 2012*, Available at: http://www.ccdcoe.org/locked-shields-2012.html (Accessed at: 11/08/2014)

NATO Cooperative Cyber Defence Centre of Excellence (2013), *Locked Shields 2013*, Available at: http://www.ccdcoe.org/locked-shields-2013.html (Accessed at: 11/08/2014)

NATO Cooperative Cyber Defence Centre of Excellence (2014), *Locked Shields 2014*, Available at: http://www.ccdcoe.org/locked-shields-2014.html (Accessed at: 11/08/2014)

NATO Cooperative Cyber Defence Centre of Excellence (2013), *Mission and Vision*, Available at: https://www.ccdcoe.org/11.html (Accessed at: 06/08/2013)

NATO Cooperative Cyber Defence Centre of Excellence (2015), *History*, Available at: http://www.ccdcoe.org/history.html (Accessed at: 10/08/2014)

NATO Parliamentary Assembly (2008), *Visit to Estonia-Finland-Sub-Committee on Transatlantic Defence and Security Co-Operation*, Available at: http://www.nato-pa.int/default.Asp?SHORTCUT=1593 (Accessed at: 03/09/2014)

NATO Parliamentary Assembly (2009), *NATO and Cyber Defence*, Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1782 (Accessed at: 04/04/2012)

Nazario, J. (2009), "Politically Motivated Denial of Service Attacks", in Czosseck, C. and Geers, K. (eds.) (2009), *The Virtual Battlefield: Perspectives on Cyber Warfare*, CCDOE Publications, Estonia: IOS Press

Neff, S. C. (2010), "A Short History of International Law", in Evans, M. (ed.) (2010), *International Law*, Oxford: Oxford University Press

Neuhold, N. (2011), "Legal Crisis Management: Lawfulness and Legitimacy of The Use of Force", in Fastenrath, U., Geiger, R., Kahn, D. E., Paulus, A., Schorlemer, S. V., Vedder, C. (eds.) (2011), *From Bilateralism to Community Interest*, Oxford: Oxford University Press

Neel, J. J. (2005), "Game theory can be used to analyze cognitive radio", *Electronic Engineering Times*, 1386

Neumann, J. von and Morgenstern, O. (1944), *Theory of Games and Economic Behavior*. Princeton, NJ: Princeton University Press

North Atlantic Defense Committee (1950), *D.C. 13 North Atlantic Treaty Organisation Medium Plan*, Available at: http://www.nato.int/docu/stratdoc/eng/a500328d.pdf (Accessed at: 06/08/2012)

North Atlantic Military Committee (1950), *M. C. 14 Strategic Guidance for North Atlantic Regional Planning*, Available at: http://www.nato.int/docu/stratdoc/eng/a500328c.pdf (Accessed at: 06/08/2012)

North Atlantic Military Committee (1952), *M. C. 14/1 Strategic Guidance for North Atlantic Regional Planning*, Available at: http://www.nato.int/docu/stratdoc/eng/a521209a.pdf (Accessed at: 06/08/2012)

Noshiravani, R. (2011), "NATO and Cyber Security: Building on the Strategic Concept", *Rapporteur Report*, Available at: http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/200511nato.pdf (Accessed at: 05/08/2012)

Nugent, J. H. and Raisinghani, M. (2008), "Bits and Bytes vs. Bullets and Bombs", in Janczewski, L. J. and Colarik, A. M. (eds.) (2008), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference

Nussbaum, A. (1947), *A Concise History of the Law of Nations*, New York: MacMilllan

O'Brien, M., *Computer Crime*, Available at: http://www.mobrien.com/computer_crime1.htm (Accessed at: 01/02/2015)

O'Connell, M. E. (2012), "Cyber Security without Cyber War", *Journal of Conflict and Security Law*, Summer, Vol. 17(2), Available at: http://jcsl.oxfordjournals.org/content/17/2/187.full#fn-46 (Accessed at: 06/02/2013)

O'Connell, M. E. and Molla, R. E. (2013), "The Prohibition on the Use of Force for Arms Control: The Case of Iran's Nuclear Program", *Penn State Journal of Law&International Affairs*, Vol. 2(2), Available at: http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1056&context=jlia (Accessed at: 15/01/2015)

Ohlin, J. D. (2011), *Nash Equilibrium and International Law*, Available at: http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1972&context=facpub (Accessed at: 20/05/2015)

Ohlin, J. D. (2015), *The Assault on International Law*, Oxford: Oxford University Press

Okhovat, S. (2011), The United Nations Security Council: Its Veto Power and Its Reform, *CPACS Working Paper*, No. 15 (1), Available at: https://sydney.edu.au/arts/peace_conflict/docs/working_papers/UNSC_paper.pdf (Accessed at: 15/04/2016)

Quenivet, N. (2005), "The World after September 11: Has It Really Changed?", *The European Journal of International Law*, Vol. 16 (3), Available at: http://www.ejil.org/pdfs/16/3/309.pdf (Accessed at: 21/05/2016)

Özdamar, Ö. (2007), "Oyun Kuramının Uluslararası İlişkiler Yazınına Katkıları", *Uluslararası İlişkiler*, Vol. 4 (15)

Palmer, D. R. (2009), "From AMF to NRF", *NATO Review*, Available at: http://www.nato.int/docu/review/2009/0902/090204/EN/index.htm (Accessed at: 08/03/2013)

Palmer, P. (2011), "Dealing With the Exceptional Pre-Crime Anti-Terrorism Policy and Practice", *Policing and Society Routledge*, Vol. 22 (4)

Paravantis, J. A. (2016), "From Game Theory to Complexity, Emergence and Agent-Based Modeling in World Politics", in Tsihrintzis, G. A., Virvou, M. and Jain, L. C. (eds.) (2016), *Intelligent Computing Systems: Emerging Application Areas*, Berlin: Springer

Parker, D. B. (1989), *Computer Crime: Criminal Justice Resource Manual*, Available at: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf (Accessed at: 02/02/2015)

Parker, D. (1998), *Fighting Computer Crime: For Protecting Information*, USA: John Wiley

Paruchuri, P., Pearce, J. P. and Kraus, S. (2008), "Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games", *AAMAS 08 Proceedings of the 7the International Joint Conference on Autonomous Agents and Multiagent Systems*, Available at: http://delivery.acm.org/10.1145/1410000/1402348/p895-paruchuri.pdf?ip=85.99.163.111&id=1402348&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2EA13CBF7F1C3C7DF4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=678714832&CFTOKEN=92564710&__acm__=1475925923_a1bb56565bf63e4fd876128226ff6692 (Accessed at: 12/09/2016)

Paruchuri, P., Pearce, J. P., Marecki, J., Tambe, M., Ordonez, F., and Kraus, S. (2008), "Efficient Algorithms to Solve Bayesian Stackelberg Games for Security Applications", P*roceedings of the Twenty-Third AAAI Conference on Artificial Intelligence*, Available at: https://www.aaai.org/Papers/AAAI/2008/AAAI08-262.pdf (Accessed at: 12/09/2016)

Pate-Cornell, E. and Guikema, S. (2002), "Probabilistic Modelling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures", *Military Operations Research*, Vol. 7(4), Available at: http://onlinepubs.trb.org/onlinepubs/archive/conferences/mb/patecornellpaper.pdf (Accessed at: 10/09/2016)

Pavel, L. (2012), *Game Theory for Control of Optical Networks*, New York: Springer Science+Business Media

Pawlak, P.(2015), "Understanding Hybrid Threats", *European Parliamentary Research Service Blog*, Available at: https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/ (Accessed at: 13/10/2016)

Perl, R. (2004), *Open For Debate: Terrorism,* New York: Benchmark Books

Peterson, J. W. (2011), *NATO and Terrorism: Organisational Expansion and Mission Transformation,* New York: Continuum

Pidgeon, N., Kasperson, R. E. and Slovic, P. (eds.) (2003), *The Social Amplification of Risk*, Cambridge: Cambridge University Press

Pita, J., Jain, M., Ordonez, F., Portway, C., Tambe,M., Western, C., Paruchuri, P. and Kraus, S. (2008), "Deployed ARMOR Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport", *AAMAS '08 Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems: Industrial*

Track, Available at: http://teamcore.usc.edu/papers/2008/AAMASind2008Final.pdf (Accessed at: 13/09/2016)

Pita, J., Jain, M., Ordonez, F., Portway, C., Tambe,M., Western, C., Paruchuri, P. and Kraus, S. (2009), “Using Game Theory for Los Angeles Airport Security”, *Al Magazine*, Available at: https://u.cs.biu.ac.il/~sarit/data/articles/AI_Magazine09.pdf (Accessed at: 13/09/2016)

Pita, J., Jain, M., Tambe, M., Ordonez, F. and Kraus, S. (2010), “Robust Solutions to Stackelberg Games: Addressing Bounded Rationality and Limited Observations in Human Cognition”, *Artificial Intelligence*, Vol. 174, Available at: http://teamcore.usc.edu/papers/2010/AIJ3.pdf (Accessed at: 12/09/2016)

Plous, S. (1993), “The Nuclear Arms Race: Prisoners’ Dilemma or Perceptual Dilemma?”, *Journal of Peace Research*, Vol. 30 (2), Available at: http://www.jstor.org/stable/pdf/425197.pdf (Accessed at: 02/09/2016)

Poel, I. and Fahlquist, J. N. (2013),” Risk and Responsibility”, in Roeser, S., Hillerbrand, R., Sandin, P., and Peterson, M. (eds.) (2013), *Essentials of Risk Theory*, London: Springer

Popescu, N. (2015), “Hybrid Tactics: Russia and the West”, *European Union Institute for Security Studies*, Issue Alert 46, Available at: http://www.iss.europa.eu/uploads/media/Alert_46_Hybrid_Russia.pdf (Accessed at: 14/10/2016)

Poundstone, W. (1993), *Prisoners Dilemma*, New York: Anchor Books

Poulsen, K. (2007), *‘Cyberwar’ and Estonia’s Panic Attack*, Available at: http://www.wired.com/2007/08/cyber-war-and-e/ (Accessed at: 30/08/2014)

Prickard, J. and MacDonald, L. (2004), “Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks*”, Journal of Information Technology Education,* Vol. 3, Available at: http://www.jite.org/documents/Vol3/v3p279-289-150.pdf (Accessed at: 08/04/2012)

Public International Law, *Lesson 5.4. Second Exception to the Prohibition on the Use of Force: Righst of Self-Defence*, Available at: https://ruwanthikagunaratne.wordpress.com/2011/04/12/article-51-un-charter/ (Accessed at: 15/01/2015)

Rapoport, A. (*Ed.*) (1974), *Game Theory as a Theory of Conflict Resolution*, Boston: D. Reidel Publishing Company

Rapoport, A. (1995), *The Origins of Violence: Approaches to the Study of Conflict*, New Jersey: Transaction Publishers

Rasmussen, M. V. (2001), “Reflexive Security: NATO and International Risk Society”, *Millennium: Journal of International Studies*, Vol. 30 (2)

Rasmussen, M. V. (2006), *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century,* Cambridge: Cambridge University Press

Rehman, S. (2013), *Estonia's Lessons in Cyberwarfare*, Available at: http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare (Accessed at: 30/08/2014)

Reichard, M. (2006), *The EU-NATO Relationship: A Legal and Political Perspective*, Aldershot: Ashgate Publishing Limited

Reinares, F. (2012), *The Evidence of Al-Qa'ida's Role in the 2004 Madrid Attack*, Available at: http://www.ctc.usma.edu/posts/the-evidence-of-al-qaidas-role-in-the-2004-madrid-attack (Accessed at: 21/08/2012)

Reisinger, H. and Golts, A. (2014), "Russia's Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence", *Research Paper*, No. 105

Renn, O., Burns, W. J., Kasperson, J. X., Kasperson, R. E. and Slovic, P. (1992), "The Social Amplification of Risk: Theoretical Foundations and Empirical Applications", *Journal of Social Issues*, Vol. 48 (4)

Renn, O. (1992), *Concept of Risk: A Classification*, Available at: https://www.researchgate.net/publication/245760840_Concepts_of_risk_A_classification (Accessed at: 16/06/2016)

Renn, O. (2008), *Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts*, Available at: http://docserver.ingentaconnect.com/deliver/connect/oekom/09405550/v17n1/s13.pdf?expires=1466950964&id=87723253&titleid=6690&accname=Guest+User&checksum=72DAC3996A08B9BDFE9ABA7BB50D3BAE (Accessed at: 15/06/2016)

Renn, O. (2008), *Risk Governance: Coping With Uncertainty in a Complex World*, London: Earthscan

Renteln, A. D. (2013), *International Human Rights: Universalism Versus Relativism*, New Orleans: Quid Pro Books

Renz, B. and Smith, H. (2016), *Russia and Hybrid Warfare: Going Beyond the Label*, Aleksanteri Papers, Available at: http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf (Accessed at: 14/10/2016)

Report of the High-Level Panel on Threats, Challenges and Change, United Nations (2004), *A More Secure World: Our Shared Responsibility*, Available at: http://www.un.org/secureworld/report.pdf (Accessed at: 28/02/2012)

Republic of Estonia Ministry of Economic Affairs and Communications, *Cyber Security*, Available at: https://www.mkm.ee/en/objectives-activities/information-society/cyber-security (Accessed at: 12/01/2015)

Richards, J. (2009), "Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security", *International Affairs Review*, Vol. XVIII, Available at: http://www.iar-gwu.org/node/65 (Accessed at: 02/10/2015)

Rieker, P. (2000), "Security, Integration and Identity Change", *Norwegian Institute of International Affairs*, Available at: https://www.ciaonet.org/attachments/11318/uploads (Accessed at: 03/01/2016)

Riigikogu (2010), *National Security Concept of Estonia*, Available at: http://www.kaitseministeerium.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf (Accessed at: 12/01/2015)

Rippl, S. (2002), “Cultural Theory and Risk Perception: A Proposal for a Better Measurement”, *Journal of Risk Research*, Vol. 5(2)

Roberts, G. W. (2000), “Humanitarian Intervention: Definitions and Criteria”, *Centre for Strategic Studies*, Vol. 3. Part 1. Available at: http://www.victoria.ac.nz/css/docs/strategic_briefing_papers/vol.3%20jun%202000/hi.pdf (Accessed at: 27/08/2012)

Rosa, E. A. (2003), “The Logical Structure of the Social Amplification of Risk Framework (SARF): Metatheoretical Foundations and Policy Implications”, in Pidgeon, N., Kasperson, R. E. and Slovic, P. (eds.) (2003), *The Social Amplification of Risk*, Cambridge: Cambridge University Press

Roscini, M. (2010), “World Wide Warfare-Jus ad bellum and the Use of Cyber Force”, *Max Planck Yearbook of United Nations Law*, Vol. 14, Available at: http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf (Accessed at: 10/05/2015)

Rousseau, D. L. (2006), I*dentifying Threats and Threatening Identities: The Social Construction of Realism and Liberalism,* Stanford: Stanford University Press.

Rousseau, D. L .and Retamero, R. G. (2007), “Identity, Power and Threat Perception: A Cross National Experiment Study”, *Journal of Conflict Resolution*, Vol. 51 (5), October, Available at: http://www.albany.edu/~dr967231/articles/RousseauJCROct2007.pdf (Accessed at: 10/08/2012)

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandiya, V. and Wu, Q. (2011), “A Survey of Game Theory as Applied to Network Security”, *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences*, Available at: http://ais.cs.memphis.edu/files/papers/Survey.pdf (Accessed at: 25/07/2016)

Russett, B. (2009), “Democracy, War and Expansion through Historical Lenses,” *European Journal of International Relations*, Vol. 15 (9)

Ruus, K. (2008), “Cyber War I: Estonia Attacked from Russia”, *European Affairs*, Vol. 9, Issue Number 1-2, Available at: http://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia (Accessed at: 10/01/2015)

Sandler, S. (1999), *The Korean War: No Victors, No Vanquished*, London: UCL Press

Sandler, T. and Enders, W. (2002), *An Economic Perspective on Transnational Terrorism*, Available at: https://www.diw.de/sixcms/detail.php/39116 (Accessed at: 10/09/2016)

Sandler, T. and Arce, D. G. (2003), “Terrorism and Game Theory”, *Simulation & Gaming*, Vol. 34/3, Available at: http://www.utdallas.edu/~tms063000/website/Terror_Games.pdf (Accessed at: 10/09/2016)

Sandler, T. and Siqueira, K. (2008), “Games and Terrorism: Recent Developments”, *Simulation&Gaming*, Available at: http://www.utdallas.edu/~tms063000/website/Sandler_Siqueira_S&Gonline.pdf (Accessed at: 10/09/2016)

Sarkar, D. (2014), *NATO adopts cybersecurity policy, says such threats, attacks no different from conventional ones,* Available at: http://www.fiercegovernmentit.com/story/nato-adopts-cybersecurity-policy-says-such-threats-attacks-no-different-con/2014-09-05 (Accessed at: 06/09/2014)

Saul, B. (2005), "Attempts to Define 'Terrorism' in International Law", *NILR*, Available at: http://www.cicte.oas.org/olat/documents/Defining%20TERRORISM%20in%20International%20Law.pdf (Accessed at: 18/07/2016)

Saul, B. (2015), "Terrorism in International and Transnational Criminal Law", *Legal Studies Research Paper*, No. 15 (83), Available at: http://ssrn.com/abstract=2663890 (Accessed at: 19/06/2016),

Schell, B. H. and Martin, C. (2004), *Cybercrime: A Reference Handbook*, California: ABC-CLIO

Schjolberg, S. (2008), *The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva*, Available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Accessed at: 05/06/2015)

Schmid, A. and Jongman, A. (2005), *Political Terrorism: A New Guide to Actors, Authors Concepts, Data Bases, Theories and Literature,* New Jersey: Transaction Publishers

Schmidt, H. K. (1958), "The Charter of the United Nations: An Instrument to Re-Establish International Peace and Security?" *Indiana Law Journal*, Vol. 33(3), Available at: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2885&context=ilj (Accessed at: 18/02/2015)

Schmitt, M. (1999), "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*

Schmitt, M. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press

Schweller, R. L. (1994), "Bandwagoning for Profit: Bringing the Revisionist State Back In", *International Security*, Vol. 19 (1), Available at: http://home.sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/17/Bandwagoning%20for%20Pofits.pdf (Accessed at: 22/05/2016)

Security Council (2004), *Resolution 1566*, Available at: http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1566%20(2004) (Accessed at: 18/06/2016)

Security Council Report (2013), *In Hindsight: The Veto*, Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/2013_11_forecast.pdf (Accessed at: 15/04/2016)

Seltzer, L. (2010), *'I LOVE YOU' Virus Turns Ten: What Have We Learned?*, Available at: http://www.pcmag.com/article2/0,2817,2363172,00.asp (Accessed at 02/10/2015)

Setty, S. (2011), "What's in a Name? How Nations Define Terrorism Ten Years After 9/11", *University of Pennsylvnia Journal of International Law*, Vol. 33 (1), Available at: https://www.law.upenn.edu/live/files/139-setty33upajintll12011pdf (Accessed at: 17/06/2016)

Shackelford, S. J. (2009), "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, Vol. 27 (1), Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil (Accessed at: 05/05/2015)

Shaw, M. (2008), *International Law,* Cambridge: Cambridge University Press

Sheean, M. (2005), *International Security and Analytical Survey*, London: Lynne Rienner Publishers

Shubik, M. (1987), "What is an application and when is a theory a waste of time?", *Management Science*, Vol. 33 (12), pp. 1511-1522: Reprinted in: Shubik, M. (1999), *Political economy, oligopoly and experimental games – the selected essays of Martin Shubik Volume One*. Cheltenham: Edward Elgar Publishing

Siegel, L.J. and Worrall, J. L. (2013), *Essentials of Criminal Justice,* Stamford: Wadsworth Cengage Learning

Silke, A. (2008), "Research on Terrorism: A Review of the Impact of 9/11 and the Global War on Terrorism", in Chen, H., Reid, E., Sinai, J., Silke, A. and Ganor, B. (eds.) (2008), *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security,* New York: Springer

Silver, D. B. (2002), "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter", *International Law Studies*, Vol. 76, Available at: https://www.usnwc.edu/Research---Gaming/International-Law/New-International-Law-Studies-(Blue-Book)-Series/International-Law-Blue-Book-Articles.aspx?Volume=76, (Accessed at: 16/05/2015)

Sim, Y. S. (2007), "International Relations& Complex System Theory", *Proceedings of the 51st Annual Meeting of the ISSS*, Available at: http://journals.isss.org/index.php/proceedings51st/article/viewFile/607/225 (Accessed at: 10/01/2016)

Skirbekk, G. and Gilje, N. (2001), *A History of Western Thought: From Ancient Greece to the Twentieth Century*, London: Routledge

Skyrms, B. (2004), The Stag Hunt and The Evolution of Social Structure, Cambridge: Cambridge University Press

Slovic, P. (2002), "Terrorism as Hazard: A New Species of Trouble", *Risk Analysis*, Vol. 22(3)

Smart, I. (1970), "The Strategic Arms Limitation Talks", *The World Today*, Vol. 26 (7)

Smith, R. K. M. (2014), *Textbook on International Human Rights*, Oxford: Oxford University Press

Snauwaert, D. T. (2004), "The Bush Doctrine and Just War Theory", *The Online Journal of Peace and Conflict Resolution*, Available at: http://www.trinstitute.org/ojpcr/6_1snau.pdf (Accessed at: 20/08/2012)

Sofaer, A. and Goodmani S. (2000), *A Proposal for an International Convention on Cyber Crime and Terrorism*, Available at: http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf (Accessed: 12/05/2012)

Sorensen, M. P. and Christiansen, A. (2013), *Ulrich Beck: An Introduction to the Theory of Second Modernity and the Risk Society*, London: Routledge

Soysal, M., Karaarslan, E., Eryol, G., and Yüce, H. (2006), "Ulaknet Bilgisayar Olaylarına Müdahale Birimi ULAK-CSIRT Deneyimi", *XI. "Türkiye'de İnternet" Konferansı Bildirileri*, Available at: http://inet-tr.org.tr/inetconf11/kitap/soysal_karaarslan_inet06.pdf (Accessed at: 13/09/2014)

State Planning Organisation (2006), *Information Society Strategy Action Plan 2006-2010*, Available at: http://www.bilgitoplumu.gov.tr/Documents/5/Documents/060700_ActionPlan.pdf (Accessed at: 11/09/2014)

Stein, G. J. (2013), "Threat Perception in International Relations", Huddy, L., Sears, D. O., and Levy, J. (eds.) (2013), *The Oxford Handbook of Political Psychology*, 2nd ed., Oxford: Oxford University Press, Available at: http://www.surrey.ac.uk/politics/research/researchareasofstaff/isppsummeracademy/instructors%20/Stein%20-%20Threat%20Perception%20in%20International%20Relations.pdf (Accessed at: 03/07/2012)

Steiner, H. J., Alston, P. and Goodman, R. (2007), I*nternational Human Rights In Context: Law, Politics, and Morals*, Oxford: Oxford University Press

Stevenson, D. (2005), *1914-1918: The History of the First World War*, London: Penguin Books

Sulaiman, R. (2005), *Information Warfare*, Available at: http://www.giac.org/paper/gsec/1870/information-warfare/103284 (Accessed at 18/02/2015)

Sungwook, K. (2014), *Game Theory Applications in Network Design*, Hershey: IGI Global

Taliharm, A. M. (2010), "Cyberterrorism: in Theory or in Practice?", *Defence Against Terrorism Review*, Vol. 3 (2)

Tambe, M. and Jain, M. (2012), "Introduction and Overview of Security Games", in Tambe, M. (2012), *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*, Cambridge: Cambridge University Press

Tams, C. J. (2009), "The Use of Force Against Terrorists, *The European Journal of International Law*, Vol. 20(2), Available at: http://www.ejil.org/pdfs/20/2/1793.pdf (Accessed at: 15/01/2015)

Tams, C. J. and Tzanakopoulos, A. (2014), "Use of Force", in Kammerhofer, J. and D'Aspremont, J. (eds.) (2014), *International Legal Positivism in a Post-Modern World*, Cambridge: Cambridge University Press

Tascan, J., Onuf, N., and Parisi, F. (1995), “International Legal Theory”, *Publication of the American Society of International Law Interest Group on the Theory of International Law,* Volume 1(1), Available at: https://law.ubalt.edu/centers/cicl/publications/docs/ILT_01_1_1995.pdf (Accessed at: 03/12/2015)

T.C. Cumhurbaşkanlığı (2010), *MGK'da Yeni Milli Güvenlik Siyaseti Belgesi Uygun Bulundu*, Available at: http://www.tccb.gov.tr/haberler/170/77759/mgkda-yeni-milli-guvenlik-siyaseti-belgesi-uygun-bulundu.html (Accessed at: 11/11/2013)

The Council of Europe (2008), *Cyberterrorism: The Use of The Internet for Terrorist Purposes*, Strasbourg: Council of Europe Publishing

The European Parliament (2011), *Defending Against Cyber Attacks*, Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611natocyberattacks_/sede150611natocyberattacks_en.pdf (Accessed at: 02/04/2012)

The Heads of State and Government (1990), *London Declaration on a Transformed North Atlantic Alliance*, Available at: http://www.nato.int/docu/comm/49-95/c900706a.htm (Accessed at: 13/08/2012)

The Heads of State and Government (1991), *The Alliance's New Strategic Concept*, Available at: http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Accessed at: 14/08/2012)

The Ministry of Transport, Maritime Affairs and Communications (2013), *National Cyber Security Strategy and Action Plan 2013-2014*, Available at: http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf (Accessed at: 15/08/2013)

The Ministry of Transport, Maritime Affairs and Communications (2016), *2016-2019 National Cyber Security Strategy*, Available at: http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf (Accessed at: 17/10/2016)

The Secretariat-General of The National Security Council (2010), *27 Ekim 2010 Tarihli Toplantı*, Available at: http://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti (Accessed at: 11/11/2013)

The Secretary of the NATO (1949), *D.C. 6/1 The Strategic Concept for the Defence of the North Atlantic Area,* Available at: http://www.nato.int/docu/stratdoc/eng/a491201a.pdf (Accessed at: 06/08/2012)

The Secretary of the NATO (1952), *M.C.* 3/5 *The Strategic Concept for the Defence of the North Atlantic Area,* Available at: http://www.nato.int/docu/stratdoc/eng/a521203a.pdf (Accessed at: 06/08/2012)

The United Nations General Assembly (1970), *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations,* Available at: http://www.un-documents.net/a25r2625.htm (Accessed at: 10/06/2014)

The United Nations General Assembly (1981), *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, A/RES/36/103,* Available at: http://www.un.org/documents/ga/res/36/a36r103.htm (Accessed at: 15/05/2015)

The United Nations General Assembly (1990), *Guidelines for the Regulation of Computerized Personal Data Files*, Available at: http://www.un.org/documents/ga/res/45/a45r095.htm (Accessed at: 20/05/2015)

The United Nations Office on Drug and Crime (2012), *The Use of the Internet for Terrorist Purposes*, United Nations; Vienna, Available at: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (Accessed at: 05/05/2015)

The United Nations Security Council, *Voting System and Records*, Available at: http://www.un.org/en/sc/meetings/voting.shtml (Accessed at: 30/08/2015)

The UN Security Council (2001), *Resolution 1368*, Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement (Accessed at: 21/05/2016)

Theiler, O. (2011), *New Threats: The Cyber Dimension*, Available at: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (Accessed at: 01/02/2012)

Thomas, J. (2008), *Cybercrime: A Revolution In Terrorism and Criminal Behavior Creates Change In The Criminal Justice System*, Available at: http://www.associatedcontent.com/article/44605/cybercrime_a_revolution_in_terrorism_html?page=2&cat=37 (Accessed at: 08/06/2013)

Thorhallson, B. (2012), "Small States in the UN Security Council: Means of Influence?", *The Hague Journal of Diplomacy*, Vol. 7, Available at: https://rafhladan.is/bitstream/handle/10802/8801/Small-States-UN-Security-Council-by-Thorhallsson.pdf?sequence=1 (Accessed at: 18/05/2016)

Thucydides (1919), *History of The Peloponnesian War Books 1-8,* Translated by Charles Froster Smith, Cambridge: Cambridge University Press

Tierney, K. T. (1999), "Toward a Critical Sociology of Risk", *Sociological Forum*, Vol. 14 (2), Available at: http://www.jstor.org/stable/pdf/684794.pdf?_=1466111013813 (Accessed at: 15/06/2016)

Tikk, E., Kaska, K., and Vihul, L. (eds.) (2010), *International Cyber Incidents: Legal Considerations*, Estonia: CCD COE Publications

Trachtenberg, M. (2003), "The Question of Realism: A Historian's View", *Security Studies,* Vol. 13 (1)

Traynor, I. (2007), "Russia accused of unleashing cyberwar to disable Estonia*"*, *The Guardian*, Available at: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (Accessed at: 08/11/2014)

Traynor, I. (2007), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *The Guardian,* Available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia (Accessed at: 30/08/2014)

Traynor, I. (2007), “Web Attackers used a Million Computers, Says Estonia”, *The Guardian*, Available at: http://www.theguardian.com/technology/2007/may/18/news.russia (Accessed at: 15/12/2014)

Trueman, C. N. (2015), *The Peace of Westphalia*, Available at: http://www.historylearningsite.co.uk/the-thirty-years-war/the-peace-of-westphalia/ (Accessed at: 06/01/2016)

Turhan, M. (2010), “Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri”, *Uzmanlık Tezi Bilgi Teknolojileri ve İletişim Kurumu*

Turocy, T. L. and Stengel, B. V. (2001), *Game Theory*, Available at: http://www.cdam.lse.ac.uk/Reports/Files/cdam-2001-09.pdf (Accessed at: 01/09/2016)

Tübitak (2010), *Ulusal Siber Güvenlik Tatbikatı Ertelendi*, Available at: http://www.uekae.tubitak.gov.tr/sid/0/cid/8153/index.htm (Accessed at: 12/11/2013)

Türkiye Bilişim Derneği (2015), “Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu”, *Nihai Rapor*, Available at: http://www.kamu-bib.org.tr/wp-content/uploads/2015/10/Kamu-B%C4%B0B-%C3%87G1-Siber-G%C3%BCvenlik-ve-Kritik-Altyap%C4%B1lar.pdf (Accessed at: 16/10/2016)

Türkiye Büyük Millet Meclisi (2012), *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu*, Available at: http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf (Accessed at: 12/09/2014)

Türkiye Büyük Millet Meclisi (2012), “Bilgi Güvenliği ve Bilişim Suçları”*, Biak Raporu*, Available at: http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf (Accessed at: 16/09/2014)

United Nations (2010), *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna*, Available at: http://www.uncjin.org/Documents/congr10/10e.pdf (Accessed at: 01/02/2015)

UNODC (2009), *International Law Aspects of Countering Terrorism*, Available at: https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf (Accessed at: 21/06/2016)

Ünal, T. (2008), “BOME 2008 Bilgi Sistemleri Güvenliği Tatbikatı: Tatbikat Sonuç Raporu, *Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü*, Available at: https://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/bilgi-sistemleri-guvenligi-tatbikati-bome-2008.html (Accessed at: 15/09/2014)

Ünver, M., Canbay, C. and Mirzaoğlu, A. G. (2011), *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*, Available at: http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/dokumanlar/sibergstmct.pdf (Accessed at: 12/09/2014)

Vatis, M. A. (2010), *The Council of Europe Convention on Cybercrime*, Available at: http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf (Accessed at: 20/05/2015)

Venkantesh, S. (2003), *Cyber Terrorism*, Delhi: AuthorsPress

Victoroff, J. (2005), “The Mind of the Terrorist: A Review and Critique of Psychological Approaches”, *The Journal of Conflict Resolution*, Vol. 49 (1), Available at: https://www.surrey.ac.uk/politics/research/researchareasofstaff/isppsummeracademy/instructors%20/The%20Terrost%20mind.pdf (Accessed at: 03/10/2015)

Viira, T. (2008), “The History of Global Harmonization on Cybercrime Legislation-The Road to Geneva”, *Meridian*, Vol.2 (1), Available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Accessed at: 11/11/2014)

von Stengel, B. and Zamir, S. (2004), “Leadership with Commitment to Mixed Strategies”, *CDAM Research Report*, Available at: http://www.cdam.lse.ac.uk/Reports/Files/cdam-2004-01.pdf (Accessed at: 11/09/2016)

Walker, C. (2006), “Cyber-Terrorism: Legal Principle and Law in the United Kingdom”, *Penn State Law Review*, Vol. 110 (3)

Walt, S. (1985), “Alliance Formation and the Balance of World Power”, *International Security*, Vol. 9 (4), Available at: http://www.christoph-rohde.de/waltallianceformationandbop1985.pdf (Accessed at: 04/07/2012)

Walt, S. M. (1987), *The Origins of Alliances*, Ithaca, NY: Cornell University Press

Walter, C. (2004), “Defining Terrorism in National and International Law”, in Walter, C., Vöneky, S., Röben, V. and Schorkopf, F. (eds.) (2004), *Terrorism as a Challenge for National and International Law: Security Versus Liberty?*, Berlin: Springer

Waltz, E. (1998), *Information Warfare Principles and Operations*, London: Artech House

Waltz, K. N. (1979), *Theory of International Politics*, New York: McGraw-Hill Publishers

Waltz, K. N. (1979), *The Anarchic Structure of World Politics*, Available at: http://people.reed.edu/~ahm/Courses/Reed-POL-372-2011-S3_IEP/Syllabus/EReadings/01.2/01.2.Waltz2005The-Anarchic.pdf (Accessed at: 10/08/2012)

Weatherall, T. (2015), “The Status of the Prohibition of Terrorism in International Law: Recent Developments”, *Georgetown Journal of International Law*, Vol. 46, Available at: https://www.law.georgetown.edu/academics/law-journals/gjil/recent/upload/zsx00215000589.PDF (Accessed at: 20/07/2016)

Webber, M. (2013), “NATO After 9/11: Theoretical Perspectives” in Hallams, E., Ratti, L. and Zyla, B. (eds) (2013), *NATO Beyond 9/11: The Transformation of the Atlantic Alliance*, Basingstoke: Palgrave Macmillan

Webber, M. and Hyde-Price, A. (2016), *Theorising NATO: New Perspectives on the Atlantic Alliance*, London: Routledge

Weber, A. M. (2003), “The Council of Europe’s Convention on Cybercrime”, *Berkeley Technology Law Journal*, Vol. 18 (1), Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj (Accessed at: 25/05/2016)

Weimann, G. (2004), “Cyberterrorism: How Real Is the Threat?”, *United States Institute of Peace Special Report No.119,* Available at: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=14122&lng=en (Accessed at: 10/03/2015)

Weimann, G. (2004), *How Modern Terrorism Uses the Internet,* Available at: http://www.usip.org/sites/default/files/sr116.pdf (Accessed at: 08/05/2015)

Weldes, J. (1999), *Constructing National Interests: The United States and the Cuban Missile Crisis,* Minneapolis: University of Minnesota Press

Wenzlaff, K. (2004), *Terrorism: Game Theory and Other Explanations*, University of Bayreuth

Williams, M. J. (2008), “(In) Security Studies, Reflexive Modernization and the Risk Society”, *Cooperation and Conflict: Journal of the Nordic International Studies Association,* Vol. 43 (1)

Williams, M. J. (2009), *NATO, Security and Risk Management: From Kosovo to Khandahar,* Oxon: Routledge

Williams, M. J. (2016), “NATO and The Risk Society: Modes of Alliance Representation Since 1991”, in Webber, M. and Hyde-Price, A. (2016), *Theorising NATO: New Perspectives on the Atlantic Alliance,* London: Routledge

Wilson, C. (2005), “Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress”, *CRS Report for Congress,* Available at: http://fpc.state.gov/documents/organization/45184.pdf (Accessed at: 01/04/2015)

Wilson, C. (2008), “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”, *CRS Report for Congress,* Available at: http://fas.org/sgp/crs/terror/RL32114.pdf (Accessed at: 11/11/2014)

Wittmann, K. (2009), “Towards a New Strategic Concept for NATO”, *NDC Forum Paper*

Wolfers, A. (1962), *Discord and Collaboration: Essays on International Politics*, Baltimore: Johns Hopkins Press

Yayla, M. (2013), “Hukuki Bir Terim Olarak Siber Savaş”, *TBB Dergisi*, Vol. 104, Available at: http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf (Accessed: 06/05/2013)

Yost, D. (1998), *NATO Transformed: The Alliance’s New Roles in International Security,* Washington: United State Institute of Peace Press

Young, R. (2006), “Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation”, *Boston College International and Comparative Law Review*, Vol. 29 (1), Available at: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1054&context=iclr (Accessed at: 02/05/2016)

Zagare, F. C. (2014), “A Game-Theoretic History of the Cuban Missile Crisis”, *Economies,* Vol. 2, Available at: http://www.mdpi.com/2227-7099/2/1/20 (Accessed at: 04/09/2016)

Zanini, M. and Edwards, S. J. A. (2001), “The Networking of Terror in the Information Age”, in Arquilla, J. and Ronfeldt, D. (2001), *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica: RAND

Zinn, J. O. and Taylor-Gooby, P. (2006), “Risk as an Interdisciplinary Research Area”, in Taylor-Gooby, P. and Taylor-Gooby, P. (eds.) (2006), Risk in Social Science, Oxford: Oxford University Press

Zinn, J. O. (2008), *Social Theories of Risk and Uncertainty: An Introduction*, Oxford: Blackwell Publishing

Zuesse, E. (2016), *NATO Says It Might Now Have Grounds to Attack Russia*, Available at: http://thesaker.is/nato-says-it-might-now-have-grounds-to-attack-russia/ (Accessed at: 12/10/2016)

3756 nolu Kanun (1991), *765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun*, Sayı: 20901, Available at: http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf (Accessed at: 10/11/2013)

5651 nolu Kanun (2007), *Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, Available at: http://www.tbmm.gov.tr/kanunlar/k5651.html (Accessed at: 15/11/2013)

Internet Sources

Estonian Embassy in Ankara, *Bir Bakışta Estonya*, Available at: http://www.estemb.org.tr/tur/estonya (Accessed at: 10/04/2014)

“About ULAKNET (Network Technologies Department)”, Available at: http://www.ulakbim.gov.tr/eng/ulaknet/ (Accessed at: 13/09/2014)

Republic of Estonia Ministry of Economic Affairs and Communications, “Cyber Security”, Available at: https://www.mkm.ee/en/objectives-activities/information-society/cyber-security (Accessed at: 12/01/2015)

The United Nations Security Council, *Voting System and Records*, Available at: http://www.un.org/en/sc/meetings/voting.shtml

The Security Council Veto List, Available at: http://research.un.org/en/docs/sc/quick/veto (Accessed at: 30/08/2015)

“About TR-CERT”, Available at: http://www.bilgiguvenligi.gov.tr/about-tr-cert.html (Accessed at: 12/09/2014)

“Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun”, Available at: http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm (Accessed at: 18/09/2014)

“Almanlar’dan Hazine’ye Siber Saldırı”, Available at: http://www.yenisafak.com.tr/gundem/turkiyeye-6-ulkeden-siber-saldiri-635531 (Accessed at: 10/10/2014

"Bomb Wounds 8 in Heart of Istanbul", Available at: http://www.nytimes.com/2011/05/27/world/europe/27turkey.html?_r=0 (Accessed at: 21/08/2012)

"Charter of the United Nations", Available at: http://www.un.org/en/documents/charter/chapter1.shtml (Accessed at: 14/01/2015)

"Convention on Cybercrime", Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Accessed at: 02/02/2015)

"Convention IV Relative to the Protection of Civilian Persons in Time of War", Available at: https://ihl-databases.icrc.org/ihl/385ec082b509e76c41256739003e636d/6756482d86146898c125641e004aa3c5 (Accessed at: 21/06/2016)

"Council of Europe Treaty Office", Available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (Accessed at: 02/02/2015)

"Crime", Available at: http://www.oxforddictionaries.com/definition/english/crime (Accessed at: 01/02/2015)

"Crime", Available at: http://www.merriam-webster.com/dictionary/crime (Accessed at: 01/02/2015)

"Cyber", Available at: http://www.oxforddictionaries.com/definition/english/cyber (Accessed at: 01/02/2015)

"Cyber Timeline", Available at: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm (Accessed at: 22/02/2015)

"Defending Against Cyber Attacks", Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf (Accessed at: 07/08/2013)

"Definition of Encryption", Available at: http://searchsecurity.techtarget.com/definition/encryption (Accessed at: 05/05/2015)

"Definition of Machiavellianism", Available at: http://www.thefreedictionary.com/Machiavellianism (Accessed at: 10/07/2012)

"Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security", Available at: http://www.iar-gwu.org/node/65 (Accessed at: 01/05/2016)

"Developing Countries", Available at: http://www.isi-web.org/component/content/article/5-root/root/81-developing (Accessed at: 01/02/2014)

"Draft Comprehensive Convention Against International Terrorism", Available at: https://www.ilsa.org/jessup/jessup08/basicmats/unterrorism.pdf (Accessed at: 19/06/2016)

"Dünya'da İnternet'in Gelişimi", Available at: http://www.internetarsivi.metu.edu.tr/tarihce.php (Accessed at: 22/09/2014)

“Dünya’nın En Etkili Bilgisayar Virüsleri”, Available at: http://www.milliyet.com.tr/fotogaleri/44071-yasam-dunyanin-en-tehlikeli-bilgisayar-virusleri/6 (Accessed at: 02/04/2015)

“Elektrik Kesintisinin Nedeni Siber Saldırı mı?”, Available at: http://www.cnbce.com/haberler/turkiye/elektrik-kesintisinin-nedeni-siber-saldiri-mi (Accessed at: 01/04/2015)

“Elektrik Kesintisi: Türkiye Bir Gün Elektrik Alamadı”, Available at: http://www.bbc.com/turkce/haberler/2015/03/150331_elektrik_rengin (Accessed at: 02/10/2015)

“Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-Attacks”, Available at: http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-ofwarfarecyberattacks/2007/05/16/1178995207414.html (Accessed at: 10/01/2015)

“Evolution of the International Arena”, Available at: http://www.mandint.org/en/evolution (Accessed at: 25/12/2015)

“Geneva Conventions*”,* Available at: http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp (Accessed at: 30/07/2012)

“Hackerler YÖK’e 123456 Şifresiyle Girmiş”, Available at: http://www.memurlar.net/haber/327857/2.sayfa (Accessed at: 10/09/2014)

“Hard Evidence: Who Uses Veto in the UN Security Council Most Often- and for What?”, Available at: http://theconversation.com/hard-evidence-who-uses-veto-in-the-un-security-council-most-often-and-for-what-29907 (Accessed at: 15/04/2016)

“International Convention for the Suppression of Financing of Terrorism”, Available at: http://www.un.org/law/cod/finterr.htm (Accessed at: 02/05/2016)

“International Covenant on Civil and Political Rights”, Available at: http://www2.ohchr.org/english/law/ccpr.htm (Accessed at: 23/08/2012)

“International Covenant on Economic, Social and Cultural Rights”, Available at: http://www2.ohchr.org/english/law/cescr.htm (Accessed at:23/08/2012)

“International Cyber and Security Conference Was Held in Ankara”, Available at: http://www.defence-turkey.com/?p=article&i=1405 (Accessed at: 08/09/2014)

“International Legal Instruments to Counter Terrorism”, Available at: http://www.un.org/terrorism/instruments.shtml (Accessed at 23/08/2012)

“Internet Usage Statistics”, Available at: http://www.internetworldstats.com/stats.htm (Accessed at: 01/06/2014)

“Istanbul Rocked by Double Bombing”, Available at: http://news.bbc.co.uk/1/hi/world/europe/3222608.stm (Accessed at: 21/08/2012)

“Istanbul Truck-Bomb Attacks Kill 27”, Available at: http://www.foxnews.com/story/0,2933,103612,00.html (Accessed at:21/08/2012)

"Keynote Speech", Available at: http://www.nato.int/cps/en/natohq/opinions_118435.htm (Accessed at: 13/10/2016)

"Nash Equilibrium and Dominant Strategies", Available at: http://economics.fundamentalfinance.com/game-theory/nash-equilibrium.php (Accessed at: 01/09/2016)

"National Cyber Shield Exercise 2012", Available at: http://www.icse2014.org/content/national-cyber-shield-exercise-2012 (Accessed at: 15/09/2014)

"National Cyber Security Exercise 2013", Available at: http://www.icse2014.org/content/national-cyber-security-exercise-2013 (Accessed at: 16/09/2014)

"National Research Institute of Electronics and Cryptology", Available at: http://uekae.bilgem.tubitak.gov.tr/en/kurumsal/national-research-institute-electronics-and-cryptology (Accessed at: 15/09/2014)

"National Security Council Members", Available at: http://www.mgk.gov.tr/en/index.php/national-security-council/nsc-members (Accessed at: 15/09/2014)

"NATO Agrees Common Approach to Cyber Defence" (2012), Available at: http://www.euractiv.com/infosociety/nato-agrees-common-approach-cyber-defence/article-171377 (Accessed at: 05/06/2013)

"NATO Approves Spearhead Force to Boost Eastern Defences", Available at: http://www.newsweek.com/nato-approves-spearhead-force-boost-eastern-defences-268656 (Accessed at: 06/09/2014)

"NATO and Cyber Defence" (2013), Available at: http://www.nato.int/cps/en/natolive/topics_78170.htm (Accessed at: 13/08/2013)

"NATO and Cyber Defence", Available at: http://www.nato.int/issues/cyber_defence/practice.html (Accessed at: 05/07/2013)

"NATO and Cyber Defense: A Brief Overview and Recent Events' Exercises", *Centre for Strategic and International Studies,* Available at: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events (Accessed at: 03/09/2014)

"NATO Cooperative Cyber Defence Centre of Excellence", Available at: http://www.ccdcoe.org/ (Accessed at: 05/04/2011)

"NATO Network Enabled Capability" (2010), Available at: http://www.nato.int/cps/de/SID-815535E4-57782C82/natolive/topics_54644.htm (Accessed at: 08/06/2012)

"NATO Sees Recent Cyber Attacks on Estonia as Security Issue", Available at: http://www.dw.de/nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579 (Accessed at: 10/01/2015)

"NATO Sets Up Rapid Reaction Force", Available at: http://www.smh.com.au/world/nato-sets-up-rapid-reaction-force-20140905-10d97x.html (Accessed at: 06/09/2014)

“NATO Summit Guide”, Available at: http://www.nato.int/lisbon2010/summit-guide-eng.pdf (Accessed at: 23/08/2012)

“NATO to Strengthen Collective Defense”, Available at: http://www.aa.com.tr/en/news/384589--nato-to-strengthen-collective-defense (Accessed at: 06/09/2014)

“Paris Attacks: What Happened on the Night”, Available at: http://www.bbc.com/news/world-europe-34818994 (Accessed at: 31/12/2015).

“Paris Terror Attack: Everything We Know on Saturday Afternoon”, Available at: http://www.telegraph.co.uk/news/worldnews/europe/france/11995246/Paris-shooting-What-we-know-so-far.html (Accessed at: 31/12/2015)

“Poland requests more NATO consultations over Russia”, Available at: http://www.reuters.com/article/2014/03/03/us-ukraine-crisis-nato-meeting-idUSBREA221VS20140303 (Accessed at: 20/08/2014)

“Prisoners’ Dilemma and the Problem of Cooperation”, Available at: http://www.baselpeaceoffice.org/sites/default/files/imce/articles/News/nuclear_prisoners_dillemma.pdf (Accessed at: 01/09/2016)

“Project on Regional Cooperation against Cybercrime in South-Eastern Europe”, Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Project_Summary_(Cybercrime_IPA)_dec_12.pdf (Accessed at: 22/09/2014)

“Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1)”, Available at: https://ihl-databases.icrc.org/ihl/WebART/470-750065 (Accessed at: 21/06/2016)

“Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol 2)”, Available at: https://ihl-databases.icrc.org/ihl/INTRO/475?OpenDocument (Accessed at: 21/06/2016)

“Quo vadis? NATO after the end of Cold War”, Available at: http://english.geopolitics.ro/quo-vadis-nato-after-the-end-of-cold-war/ (Accessed at: 03/01/2016)

“Report of the Official Account of the Bombings in London on 7th July 2005”, Available at: http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf (Accessed at: 21/08/2012)

“Security Council Veto List”, Available at: http://research.un.org/en/docs/sc/quick (Accessed at: 26/04/2016)

“Siber Güvenlik Kurulu”, Available at: http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/siberguvkurulu.php (Accessed at: 18/09/2014)

“Siber Güvenlik Kurulu Kuruldu”, Available at: http://www.ntvmsnbc.com/id/25391671 (Accessed at: 18/09/2014)

"Siber Güvenlik Tatbikatı Başladı", Available at: http://www.sabah.com.tr/Teknoloji/Haber/2013/01/10/siber-guvenlik-tatbikati-basladi (Accessed at: 16/09/2014)

"Siber Tatbikat Başladı", Available at: http://www.ntvmsnbc.com/id/25175053/ (Accessed at: 15/09/2014)

"Siber Kalkan Tatbikatı 2012 Tamamlandı", Available at: http://www.tk.gov.tr/sayfa.php?ID=101 (Accessed at: 15/09/2014)

"Siber Kalkan Açıldı", Available at: http://ekonomi.haberturk.com/teknoloji/haber/746971-siber-kalkan-acildi (Accessed at: 15/09/2014)

"Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ", Available at: http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (Accessed at: 18/10/2014)

"Siber Saldırılara Müdahale Merkezi Kurulacak", Available at: http://www.ntvmsnbc.com/id/25450250/ (Accessed at: 19/09/2014)

"Taner Yıldız: Siber Saldırı mıdır? Söyleyemem!", Available at: http://www.radikal.com.tr/turkiye/taner_yildiz_siber_saldiri_midir_soyleyemem-1325196 (Accessed at: 01/04/2015)

"Terörle Mücadele Kanunu", Available at: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf (Accessed at: 21/09/2014)

"Terrorist Bomb Trains in Madrid", Available at: http://www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid (Accessed at: 21/08/2012)

"The Alliance's New Strategic Concept 1991", Available at: http://www.nato.int/cps/en/natohq/official_texts_23847.htm (Accessed at: 05/05/2016)

"The Constitution of the Republic of Turkey", Available at: http://www.hri.org/docs/turkey/part_iii_2.html (Accessed at: 15/09/2014)

"The Covenant of the League of Nations", Available at: http://avalon.law.yale.edu/20th_century/leagcov.asp (Accessed at: 29/07/2012)

"The definition of Asymmetric Warfare", Available at: http://dictionary.reference.com/browse/asymmetric+warfare (Accessed at: 01/07/2014)

"The definition of DDOS", Available at: http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html (Accessed at: 01/07/2014)

"The History of Cyber Attacks: A Timeline", *NATO Review*, Available at: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (Accessed at: 11/11/2013)

"The Islamic State Militant Group Claims Responsibility for Paris Attacks in Which At Least 128 Die", Available at: http://www.euronews.com/2015/11/14/explosion-in-paris-near-stade-de-france-conversely-two-dead-seven-wounded-in/ (Accessed at: 31/12/2015)

"The list of IP numbers", Available at: http://krezi.livejournal.com/168695.html (Accessed at: 15/01/2015)

"The Meaning of Cyber", Available at: http://www.thefreedictionary.com/cyber- (Accessed at: 01/02/2015)

"The North Atlantic Treaty", Available at: http://www.nato.int/cps/en/natolive/official_texts_17120.htm (Accessed at: 23/08/2012)

"The Prague Summit and NATO's Transformation", (2003), Available at: http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf (Accessed at: 03/02/2012)

"The Security Council Veto List", Available at: http://research.un.org/en/docs/sc/quick/veto (Accessed at: 30/08/2015)

"The Softest Target", Available at: http://www.guardian.co.uk/world/2003/nov/23/turkey.terrorism (Accessed at: 21/08/2012)

"The Statute of the International Court of Justice", Available at: http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0#CHAPTER_II (Accessed at: 22/08/2012)

"The Terrorism Act 2000", Available at: http://www.legislation.gov.uk/ukpga/2000/11/contents (Accessed at: 18/04/2016)

"The title 22 of the U.S. Code", Available at: http://www.state.gov/documents/organization/65464.pdf (Accessed at: 20/08/2012)

"The United Nation Charter", Available at: http://www.un.org/en/documents/charter/chapter1.shtml (Accessed at: 04/08/2012)

"The Universal Declaration of Human Rights", Available at: http://www.un.org/en/documents/udhr/ (Accessed at: 23/08/2012)

"The 2004 Madrid Bombings", Available at: http://www.guardian.co.uk/world/2007/oct/31/spain.menezes (Accessed at: 21/0/2012)

"Timeline of Terror: How the Horror Unfolded in Paris", Available at: http://www.nbcnews.com/storyline/paris-terror-attacks/timeline-terror-how-horror-unfolded-paris-n463561 (Accessed at: 31/12/2015)

"Title 18 of the U.S. Code", Available at: https://www.law.cornell.edu/uscode/text/18/2331 (Accessed at: 18/04/2016)

"Toward Perpetual Peace", Available at: http://www2.hawaii.edu/~freeman/courses/phil320/21.%20Perpetual%20Peace.pdf (Accessed at: 05/01/2016)

"TSK'da Siber Savunma Merkezi Başkanlığı Kuruldu", Available at: http://www.radikal.com.tr/turkiye/tskda_siber_savunma_merkezi_baskanligi_kuruldu-1117859 (Accessed at: 13/11/2013)

"TSK Siber Savunma Merkezi Başkanlığı Kuruldu", Available at: http://www.btnet.com.tr/64622-tsk-siber-savunma-merkezi-baskanligi-kuruldu.html (Accessed at: 13/11/2013)

“TSK’da Siber Savunma Komutanlığı”, Available at: http://gundem.bugun.com.tr/tskda-siber-savunma-komutanligi-haberi/215064 (Accessed at: 13/11/2013)

“Turkey’s Relations with NATO”, Available at: http://www.mfa.gov.tr/nato.en.mfa (Accessed at: 07/08/2014)

“Turkish Army’s New Cyber Defence Unit”, Available at: http://www.aa.com.tr/en/news/124195--turkish-armys-new-cyber-defense-unit (Accessed at: 08/09/2014)

“Turkish Criminal Procedures Code”, Available at: http://www.justice.gov.tr/basiclaws/cmk.pdf (Accessed at: 19/09/2014)

“Türk Bankaları Siber Saldırı Altında”, Available at: http://www.hurriyet.com.tr/teknoloji/27037274.asp (Accessed at: 10/10/2014)

“Türkiye’de Büyük Çapta Elektrik Kesintisi: Siber Saldırı İhtimali Araştırılıyor”, Available at: http://tr.sputniknews.com/turkiye/20150331/1014730458.html (Accessed at: 01/04/2015)

“Türkiye’ye en çok bu 3 ülkeden siber saldırı geliyor”, Available at: http://www.hurriyet.com.tr/teknoloji/26989400.asp (Accessed at: 10/10/2014)

“Türkiye’ye 6 ülkeden siber saldırı”, Available at: http://www.yenisafak.com.tr/gundem/turkiyeye-6-ulkeden-siber-saldiri-635531 (Accessed at: 10/10/2014)

“Türkiye’ye Siber Saldırı”, Available at: http://www.hurriyet.com.tr/teknoloji/20440458.asp (Accessed at: 15/11/2013)

“*Türkiye de “Sanal Suçlar Sözleşmesini “ İmzaladı*”, Available at: http://www.bilisimdergisi.org/s127/pdf/10-13.pdf (Accessed at: 12/11/2013)

“Türkiye’de Siber Kalkan Koruması”, Available at: http://www.turkishny.com/technology/91-technology/90755-turkiyeye-siber-kalkan-korumasi/pdf (Accessed at: 15/09/2014)

“Türkiye’ye Siber Saldırı Tehdidi”, Available at: http://www.dunya.com/turkiyeye-siber-saldiri-tehdidi-152944h.htm (Accessed at: 10/09/2014)

“Turkey Logs on to Europe’s Internet Treaty”, Available at: http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkey-signs-cybercrime-convention-promises-international-cooperation-2010-11-10 (Accessed at: 12/11/2013)

“Turkish Academic Network and Information Centre”, Available at: http://www.ulakbim.gov.tr/eng / (Accessed at: 13/09/2014)

“ULAK-CSIRT”, Available at: http://csirt.ulakbim.gov.tr/eng/ (Accessed at: 13/09/2014)

“Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar”, Available at: http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (Accessed at: 12/11/2013)

“Ulusal Siber Güvenlik Stratejisi ve 2015-2016 Eylem Planı 1 Ortak Çalıştayı Gerçekleşti”, Available at: http://sge.bilgem.tubitak.gov.tr/tr/haber/ulusal-siber-guvenlik-stratejisi-ve-2015-2016-eylem-plani-1-ortak-akil-calistayi-gerceklesti (Accessed at: 16/10/2016)

“Ulusal Siber Güvenlik Tatbikatı 2011”, Available at: http://www.tk.gov.tr/sayfa.php?ID=28 (Accessed at: 15/09/2014)

“Ulusal Siber Güvenlik Tatbikatı 2013”, Available at: http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2013.php (Accessed at: 16/09/2014)

“Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı”, Available at: http://www.btnet.com.tr/17477-ulusal-siber-guvenlik-tatbikati-basariyla-tamamlandi.html (Accessed at: 15/09/2014)

“2. Ulusal Siber Güvenlik Tatbikatı”, Available at: http://www.ubak.gov.tr/BLSM_WIYS/UBAK/tr/BELGELIK/guncel_haber/20130110_141118_204_1_2561.html (Accessed at: 16/09/2014)

“2. Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı”, Available at: http://www.tk.gov.tr/sayfa.php?ID=153 (Accessed at: 18/09/2014)

“Ve Türkiye’ye Siber Saldırı Başladı”, Available at: http://www.posta.com.tr/guncel/HaberDetay/Ve_Turkiye_ye_siber_saldiri_basladi.htm?ArticleID=75372%20%20%20%20%20%20%20%20%20%20&Date=19.04.2010&PageIndex=2 (Accessed at: 10/09/2014)

“War in Afghanistan (2001-present)”, Available at: http://www.saylor.org/site/wp-content/uploads/2011/06/War-in-Afghanistan-2001-Present.pdf (Accessed at: 21/08/2012)

“What is NATO”, Available at: http://www.nato.int/nato-welcome/ (Accessed at: 12/10/2016)

“What is SCADA”, Available at: https://www.inductiveautomation.com/what-is-scada (Accessed at: 16/09/2014)

“Why is Turkey in NATO”, Available at: http://www.ibtimes.com/why-turkey-nato-704333 (Accessed at: 07/08/2014)

“Who We Are”, Available at: http://www.tubitak.gov.tr/en/about-us/content-who-we-are (Accessed at: 12/09/2014)

“YÖK’e Siber Saldırı”, Available at: http://www.gazetevatan.com/yok-e-siber-saldiri--503255-gundem/ (Accessed at: 10/09/2014)

YÖK’e Siber Saldırı”, Available at: http://beyazgazete.com/video/anahaber/cnn-turk-12/2013/01/11/yok-e-siber-saldiri-364616.html (Accessed at: 10/05/2014)

“25 Biggest Cyber Attacks in History”, Available at: http://list25.com/25-biggest-cyber-attacks-in-history/ (Accessed at: 22/02/2015)

“2005: Bomb Attacks on London”, Available at: http://news.bbc.co.uk/onthisday/hi/dates/stories/july/7/newsid_4942000/4942238.stm (Accessed at: 21/08/2012)

“7 July 2005 London Bombings”, Available at: http://www.martinfrost.ws/htmlfiles/london_bombs2.html (Accessed at: 21/08/2012)

“79 İlde Elektrik Kesintisinin Nedeni Siber Saldırı mı?”, Available at: http://www.aktifhaber.com/79-ilde-elektrik-kesintisinin-nedeni-siber-saldiri-mi-1147527h.htm (Accessed at: 01/04/2015)

“1969 Vienna Convention on the Law of Treaties”, Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf (Accessed at: 16/05/2015)