Universitat Autònoma de Barcelona

THE RIGHT OF SELF-DEFENCE AGAINST CYBER ATTACKS BY STATES AND NON- STATE ACTORS

HAMED RAFIGHDOUST

FACULTAT DE DRET

THE RIGHT OF SELF-DEFENCE AGAINST CYBER ATTACKS BY STATES AND NON-STATE ACTORS

Tesi presentada per aspirar al títol de Doctor per

HAMED RAFIGHDOUST

Realitzada sota la direcció del Dr. Jaume Munich i Gasa
Professor Titular de Dret Internacional Públic i Relacions Internacionals
Universitat Autònoma de Barcelona

Tutora: Dra. Esther Zapater Duque
Professora Titular de Dret Internacional Públic i Relacions Internacionals
Universitat Autònoma de Barcelona

Bellaterra, 2 de juliol de 2018

ABREVIATIONS

A. **PERIODICALS**

AEDI……Anuario Español de Derecho Internacional

AFDI……Annuaire Français de Droit International

AJIL……American Journal of International Law

BOE……Boletín Oficial del Estado

BYIL……British Yearbook of International Law

CYIL……Canadian Yearbook of International Law

EJIL……European Journal of International Law

GYIL……German Yearbook of International Law

HILJ……Harvard International Law Journal

ICLQ……International and Comparative Law Quarterly

JCSL……Journal of Conflict and Security Law

JUFIL……Journal on the Use of Force and International Law

LJIL……Leiden Journal of International Law

MJIL……Michigan Journal of International Law

NILR……Netherlands International Law Review

NJIL……Nordic Journal of International Law

NYIL……Netherlands Yearbook of International Law

OJEU……Official Journal of the European Union

RCADI……Recueil des Cours de l'Académie de Droit International de La Haye

REDI……..Revista Española de Derecho Internacional

RGDIP……Revue Générale de Droit International Public

RIAA……..Report of International Arbitral Awards

VJTL ……..Vanderbilt Journal of Transnational Law

YJIL……..Yale Journal of International Law

B. **OTHER ABREVIATIONS**

CEO……..Cyber Effects Operations

COE ……..Council of Europe

CNA…… Computer Network Attacks

CND…… Computer Network Defence

CNE…… Computer Network Exploitation

CNO…… Computer Network Operation

CUP……..Cambridge University Press Excellence

DCO…… Defensive Cyberspace Operation

DDoS ……..Distributed Denial-of-Service

DoD……..Department of Defence

DRC……Democratic Republic of Congo

ECHR……European Court of Human Rights

GGE ……Groups of Governmental Experts

HPCR……High Pressure Common Rail

EU…… European Union

ICC.....International Criminal Court

ICJ.....International Court of Justice

ICRC.....International Committee of the Red Cross

ICT.....Information and Communications Technologies

ICTY.....International Criminal Tribunal for the former Yugoslavia

IDI.....Institut de Droit International

IHL.....International Humanitarian Law

IIFFMCG .....Independent International Fact-Finding Mission on the Conflict in Georgia

ILA.....International Law Association

ILC.....International Law Commission

NATO.....North Atlantic Treaty Organization

NATO CCDCOE.....NATO Cooperative Cyber Defence Centre of Exellence

NCI .....National Critical Infrastructure

NPT.....Treaty on the Non-Proliferation of Nuclear Weapons

NSS.....National Security Strategy

OAS.....Organization of American States

OCO..... Offensive Cyberspace Operations

OECD.....Organization for Economic Cooperation and Development

OSCE.....Organization for Security and Cooperation in Europe

OUP.....Oxford University Press

UK.....United Kingdom

UN.....United Nations

UNCIO.....United Nations Conference of International Organization

UN GGE.....United Nations Governmental Group of Experts

UNGA……United Nations General Assembly

UNSC……United Nations Security Council

UNSG.....United Nations Secretary General

US……United State of America

USSR.....Union of Soviet Socialist Republics

RULAC……Rule of Law in Armed Conflicts

SCO.....Shanghai Cooperation Organization

WMD..... Weapon of Mass Destruction

TABLE OF CONTENTS

CHAPTER II

THE RIGHT OF SELF-DEFENCE IN INTERNATIONAL LAW

CHAPTER III

THE RIGHT OF SELF-DEFENSE AGAINST CYBER OPERATIONS BY STATES AND NON-STATE ACTORS

INTRODUCTION

A. **Delimitation of the object**

Undoubtedly, technological advance are shaping the development of our society. The cyber technology has lead us to the so-called cyber society characterized by new economic, *socio-cultural* and political guidelines. *Because* of the current possibilities offered by technology numerous norms, both internal and international, are rapidly becoming obsolete, being unable to give answer to the new issues regarding to the cyber space. In fact, nowadays International Law has to cope with problems that were unimaginable at the moment its rules were first adopted, in particular, the regulation relating to the prohibition of the threat or the use of force and the exception of the right of self-defence. Neither the States nor the international organizations have remained aloof from the new legal challenges that have emerged around cyber technology.

In this regard, actual and potential threats emerging from activities in cyberspace are matters of substantial concerns among States, especially in developed States that reasonably are more vulnerable to such threats based on excessive technological dependency[1].

In this sense, the US in its *Assessment of International Legal Issues in Information Operations* expressed its concern over cyber space threats where

> "The attacker may be a foreign State, an agent of a foreign State, an agent of a non-governmental entity or group, or an individual acting for purely private purposes. The equipment necessary to launch a computer network attack is readily available and inexpensive, and access to many computer systems can

[1] "An excessive computer dependency creates a special vulnerability", DINSTEIN, Y., "Computer network attacks and self-defense", in SCHMITT, M. N., O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, monographic published in *International Law Studies*, 76(1), 2002, p. 99-119, at p. 105.

> be obtained through the Internet or another network to which access is easily obtained"[2].

Furthermore, former President Obama issued an *Executive Order* whose *Section 1* explicitly expressed its concerns that "the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront"[3].

In the framework of the United Nations (UN), the Russian Federation introduced in 1998 a Draft Resolution in the First Committee of the United Nations General Assembly (UNGA), where pointed out its

> "concern that these technologies and means may potentially be used for purposes incompatible with the objectives of ensuring international security and stability and the observance of the principles of non-use of force, non-interference in internal affairs and respect for human rights and freedoms"[4].

Hence, the problem of cyber space threat has been on the UN agenda since the Russian Federation first introduced this Draft Resolution. From then on, concern on cyber space activities has been reflected in the UNGA Resolution 57/239 of 2002, where it noted, "as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all"[5]. Also, both in the UNGA Resolution 58/199 of 2003 and in the UNGA

---

[2] US, DoD*, An Assessment of International Legal Issues in Information Operations*, May 1999, p. 5.

[3] US, *Executive Order-Improving Critical Infrastructure Cybersecurity*, 12 February, 2013, available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; see also CROOK, J. R., "US efforts to enhance cybersecurity and to counter international theft of trade secrets", *AJIL*, 107(2), 2013, p. 447-449.

[4] UNGA, Doc. A/C.1/53/3 "Role of science and technology in the context of international security, disarmament and other related fields", 30 September 1998, p. 3.

[5] UNGA, Resolution 57/239 "Creation of a global culture of cybersecurity", 20 December 2002, p. 2.

Resolution 64/211 of 2009, there has been a special emphasis on the protection of critical information infrastructures from cyber threats[6].

Furthermore, there have been annual reports by the United Nations Secretary-General (UNSG) to the UNGA with the views of UN Member States on the *Developments in the field of information and telecommunications in the context of international security*[7]. In this regard some States, such as Germany, affirmed that

> "process control systems for critical infrastructures have proven particularly vulnerable to malicious ICT operations. The risks of uncontrollable collateral damage on a global scale are high, including the infection of industrial control systems with potentially physical destructive effects. A single cyber attack against core telecommunication infrastructure could cause more global disruption than a single physical attack"[8].

Moreover, the UK recognized "cyberspace as a fundamental element of securing critical national and international infrastructure and an essential foundation for economic and social activity online. Actual and potential threats posed by activities in cyberspace continue to be of great concern"[9].

To cope with these concerns, in 2011 a law adopted by Spain made an important step forward towards the protection of the most critical infrastructures[10] and, in 2016, it also gave clear support to the process of achieving an international consensus on cyber security,

---

[6] UNGA, Resolution 58/199 "Creation of a global culture of cybersecurity and the protection of critical information infrastructures", 23 December 2003; and Resolution 64/211 "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", 21 December 2009.

[7] Among others, UNGA, Doc. A/68/156, of 16 July 2013; UNGA, Doc. A/69/112, of 30 June 2014; UNGA, Doc. A/70/172, of 22 July 2015; UNGA, Doc. A/71/172, of 19 July 2016; and UNGA, Doc. A/72/315, of 11 August 2017 on "Developments in the field of information and telecommunications in the context of international security".

[8] PERMANENT MISSION OF FEDERAL REPUBLIC OF GERMANY TO THE UNITED NATIONS, Note No. 516/2012, 5 November 2012.

[9] UNGA, Doc. A/72/315 "Developments in the field of information and telecommunications in the context of international security", 11 August 2017, p. 25.

[10] *Ley 8/2011, por la que se establecen medidas para la protección* de *infraestructuras críticas*, 28 April 2011.

asserting that "States should continue reflecting on how the principles and norms of International Law, especially those relating to the threat or use of force, humanitarian law and protection of the fundamental rights and freedoms of individuals, should be interpreted and applied in cyberspace"[11].

Since 2004, the UN has settled some *Groups of Governmental Experts* (GGE) to examine the existent and potential threats from the cyber-sphere and possible cooperative measures to address them. The First 15-member Group was established in 2004 but it did not agree on a substantive report. The first successful UN GGE report, issued by the Second Group in 2010, emphasized

> "The growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Since ICTs are inherently dual-use in nature, the same technologies that support robust e-commerce can also be used to threaten international peace and national security"[12].

The Third UN GGE report, submitted to the UNGA in June 2013, stressed that "threats to individuals, businesses, national infrastructure and Governments have grown more acute and incidents more damaging. The sources of these threats comprise both State and non-State actors"[13].

The Fourth UN GGE, established in 2015 with 20 experts including all UNSC Permanent members, affirmed in its report that "the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs

[11] UNGA, Doc. A/71/172 "Developments in the field of information and telecommunications in the context of international security", 19 July 2016, p. 20.

[12] UNGA, Doc. A/65/201 "Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security", 30 July 2010, p. 2.

[13] UNGA, Doc. A/68/98 "Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security", 24 June 2013, p. 6.

or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security"[14]. The Fifth UN GGE, in its fourth and final session on 19-23rd June 2017, ended without consensus on its final report.

These reports introduced that existing International Law applies to the digital space, and developed norms and principles of responsible behavior of States in cyberspace. While such UN GGE reports carry significant influence in the field of global cyber security, the Group's future is uncertain. In its absence, it seems States may lean towards bilateral agreements, a trend which has become particularly prevalent in the last years[15].

Moreover, the UN GGE reports in 2013 and 2015 respectively, were unanimously adopted by UNGA Resolutions 68/243 of 2013 and 70/237 of 2015 expressing their concern that "these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields"[16].

In addition to that, with the aim of establishing confidence and security in the use of Information and Communication Technologies (ICT), the International Telecommunications Union (ITU) launched in 2007 the *Global Cybersecurity Agenda* (GCA) as a framework for international cooperation in this field.

Furthermore, the challenges in cyber space have been engaged in other international organizations such as the Organization for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), the European Union (EU), the Organization for Economic Cooperation and Development (OECD) and the Council of Europe (COE).

---

[14] UNGA, Doc. A/70/174 "Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security", 22 July 2015, p. 6.

[15] "Digital policy trend in June", *Geneva Digital Watch, 22, 30 June 2017,* available at https://dig.watch/DWnewsletter22, [visited on 24 April 2018].

[16] UNGA, Resolution 68/243 "Developments in the field of information and telecommunications in the context of international security", 27 December 2013, p. 2; and Resolution 70/237 "Developments in the field of information and telecommunications in the context of international security", 23 December 2015, p. 2.

The OSCE Parliamentary Assembly (PA) in 2008 adopted a Resolution on *Cyber Security and Cyber Crime* where it recognized that "threats originating from cyber space are one of the most serious security challenges of present time, which can jeopardize the way of life of modern societies and the whole of civilization"[17]. Moreover, in the *Minsk Declaration* it also mentioned its concern about the "ongoing security challenges throughout the OSCE area, including cyber security threats and violent extremism" and urged to take measures "to enhance cyber security between States, to prevent tension and conflicts stemming from the use of information and communication technologies, and to protect critical infrastructure from cyber threats"[18]. Later on, in the Lisbon conference on *Digital Resilience of a Democratic State*, the OSCE PA emphasized how protections against cyber threats must build trust and uphold fundamental freedoms[19].

Cyber operations have been part of NATO's political agenda since the Prague Summit in 2002 and the cyber attacks against Estonia in 2007 may be seen as initiating the gradual shift in the attention the Alliance has paid to cyber defence; thus in 2008, was prepared the *NATO's First Cyber Defence Policy*. At the Lisbon Summit in 2010, cyber defence was included in *NATO's Strategic Concept*[20]. In 2013, NATO Cooperative Cyber Defence Centre of Excellence invited an international group of approximately twenty experts to set up principles to confront the threats of cyber attacks referred to in *Tallinn Manual*. There, it focused on the most disruptive and destructive cyber operations, which can be qualified as *armed attacks* and, therefore, allow States to respond in self-defence[21]. *Tallinn Manual* was

[17] OSCE PA, "Resolution on Cyber Security and Cyber Crime", *Astana Declaration of the OSCE Parliamentary Assembly and Resolutions adopted at the Seventeenth Annual Session*, 3 July 2008, par. 17.

[18] OSCE PA, *Minsk Declaration and Resolutions adopted by the OSCE Parliamentary Assembly at the Twenty-sixth Annual Session*, 9 July 2017, pars 1 and 38.

[19] OSCE PA, Lisbon Conference on *Digital Resilience of a Democratic State*, 8 May 2018, available at http://www.oscepa.org/news-a-media/press-releases/2853-protections-against-cyber-threats-must-build-trust-and-uphold-fundamental-freedoms-say-osce-parliamentarians-at-lisbon-conference, [visited on 8 June 2018].

[20] NATO, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted by Heads of State and Government at the NATO Summit in Lisbon, 19 November 2010, available at https://www.nato.int/cps/en/natohq/official_texts_68580.htm, [visited on 22 May 2018].

[21] INTERNATIONAL GROUP OF EXPERTS, *Tallinn Manual on the International Law applicable to cyber warfare*. CUP, 2013; hereinafter quoted as *Tallinn Manual.* The Group of Experts included only military and academic lawyers and technical experts from a few Western State; in effect of 23 members of such Group, nine,

updated in 2017 by *Tallinn Manual 2.0,* which examines the international legal framework applicable to cyber operations and explores the general principles of International Law[22].

On 5 September 2014, a new enhanced Cyber Defence Policy was approved at the *Wales Summit* where it affirmed that a major digital attack on a member State could be covered by article 5 NATO Treaty[23], and it emphasized on a "dialogue and cooperation between NATO and the EU]...[to address issues of common concern, including security challenges like cyber defence, the proliferation of weapons of mass destruction, counter-terrorism and energy security"[24].

In the light of the common challenges on cyber space that both the NATO and the EU have to confront, a *Joint Declaration* was adopted on 8th July 2016 to establish cooperation in the field of cyber security and defence as a strategic priority[25]. Following this Declaration, the Council of the EU approved a *Conclusion* on its implementation on 6th December 2016[26].

In fact, since the nineteenth century, the EU has been developing activities in the field of cyber space and it certainly took a conscious decision to developing a fully-fledged approach to cyber security due to the increasing numbers of cyber-attacks on individuals,

---

including M. N. Schmitt the Project Director's, where from the US, while none of them "from States that are reportedly heavily involved in cyber operations, both as authors and targets, such as Russia, China, Iran, or Israel", *cfr.* ROSCINI, M., *Cyber operations and the use of force in International law: Identifying the problem and the applicable law*, OUP, 2014, p. 31. However, *Tallinn Manual* theoretically represents only the views of the Group of Experts, but not of NATO, the NATO CCD COE, its sponsoring States, nor any other State or organization.

[22] INTERNATIONAL GROUP OF EXPERTS, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, CUP, 2017; hereinafter quoted as *Tallinn Manual 2.0.*

[23] NATO, *Wales Summit Declaration*, 5 September 2014, par. 72, available at https://www.nato.int/cps/ic/natohq/official_texts_112964.htm, [visited on 6 June 2018]

, par. 104.*Ibid* [24].

[25] NATO-EU, *Joint Declaration; by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, of 8 July 2016 available at https://ccdcoe.org/eu-nato-relations-hand-hand-against-cyberattacks.html,, [visited on 4 May 2018] ; see also TRINBERG, L., "EU-NATO relations: hand in hand against cyber attacks", 13 January 2017, available at https://ccdcoe.org/eu-nato-relations-hand-hand-against-cyberattacks.html, [visited on 6 May 2018].

[26] COUNCIL OF THE EU, *Council Conclusion on the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the NATO*, 6 December 2016, available at http://www.consilium.europa.eu/en/press/press-releases/2016/12/06/eu-nato-joint-declaration/, [visited on 8 June 2018].

companies and critical infrastructures. In this regard, the Council of the EU passed a decision on attacks against information system in 2005[27], and the European Commission and HREU publishing their first cyber security strategy in 2013[28]. In terms of legislation, in 2016 the EU adopted its most ambitious instrument to date, the *Network and Information Security* (NIS) *Directive*, which has introduced incident reporting obligations for the private sector, including operators of essential services and digital service providers[29]. In 2017, the Council of the EU approved a *Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* with the ultimate aim of reinforcing the EU's activities in this field and potentiating a more coordinated response in case of cyber-attacks against European targets[30].

Finally, the Council of Europe, as a response to the increase of the cyber threats, adopted the *Convention on cyber-crime* with the purpose of harmonizing national laws on this subject. In this regard, it convinced of the necessity to pursue a common criminal policy, aiming at the protection of society against cyber-crime by adopting appropriate legislation and fostering international cooperation[31].

Obviously, it is impossible to attempt to address in this research all the issues emerging on cyber activities, because of the widespread implementation of cyber operations. Therefore, it is necessary to delimit the object of our investigation. In this sense, our study is not

---

[27] COUNCIL OF THE EUROPEAN UNION, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJEU L 69*, 16 March 2005, p. 67.

[28] EUROPEAN COMMISSION and HREU, *Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN (2013) 1 final, 7 February 2013, available at https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf,]visited on 6 July 2017[.

[29] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJEU L 194*,19 July 2016, p. 1.

[30] COUNCIL OF THE EU, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),* 7 June 2017, available at http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf,]visited on 8 June 2018[; see CARRAPICO, H.; BARRINHA, A., "European Union cyber security as an emerging research and policy field", *European Politics and Society*, 19(3), 2018, p. 299-303, available at https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430712, [visited on 8 June 2018].

[31] COUNCIL OF EUROPE, *Convention on Cybercrime*, 23 November 2001.

comprehensive and does not deal with, for instance, international criminal law, trade law, intellectual property, private International Law or domestic law. This research is upon Public International Law related to cyber activities, particularly those that, according to article 51 of the UN Charter, give a victim State the right to act in self-defence, especially when the attackers are non-State actors. Thus, we are not going to cope with cyber activities related to cyber warfare, cyber responsibility, international telecommunications law, human rights, diplomatic law, law of the sea, air law or space law.

B. **Purpose of the research**

In the last decades, there has not been an area which has developed faster than cyber technology. As a result, it has given rise to new challenges for the International Law. However, at the same time, many objectives to successfully deal with these challenges are arising, being the guarantee of peace and security the most important.

Due to the lack of consensus among States to adopt new norms, at least until now, and the dynamic rather than static features of International Law, in this research we are going to find out in what measure can the existing principles and rules of International Law be adopted to cope with the new threats raised around the cyber technology. Then, International law must remain relevant to modern conflicts on cyber space with the aim of confronting malicious cyber activities against State sovereignty. Thus, it has to be respected to ensure certainty, peace and stability in the international order. If it was considered irrelevant or ignored by cyber actors, the world would be less safe.

The absence of specific norms, customary principles or State practice regulating cyber operations in International Law, drives many scholars to pursue answers based on analogies and to elaborate proposals of new rules. Our task, in this research, will be to focus on finding out in which way has the International Law been modified to cope with cyber activities threats.

In order to analyze the exercise of the right of self-defence against cyber-attacks, the first question to ask is whether a cyber-operation can violate the principle of the *prohibition of*

the threat or the use of force, particularly when such operations give rise to high level of economic and political intensity.

One of the most significant requirements to exercise the right of self-defence is the existence of an *armed attack* in the sense of article 51 of the UN Charter. Therefore, one of the fundamental questions in our investigation would be whether a cyber-attack can constitute an armed attack and, if so, under which conditions can cyber operations amount to an armed attack to justify resorting to the right of self-defence. In this regard, it is important to stress that the armed attack is found among the most grave forms of the use of force. Then, it is relevant to analyze when a series of *low intensity cyber-attacks*, which individually do not rise to the level of an *armed attack*, cumulatively can amount to an armed attack to exercise the right of self-defence.

The increase of military or cyber operations by non-State actors constitute serious threats to the State sovereignty and arise the issue of whether cyber operations by non-State actors with high gravity can justify the right of self-defence against such actors, especially when any State is substantially involved in such operations. Moreover, it raises the question of whether States have the authorization to use kinetic weapons in the right of self-defence in response to cyber operations that amount to an armed attack.

In relation to other requirements, particularly to the immediacy condition, we attempt to give appropriate answer whether in front of an imminent cyber-attack is, in contemporary International Law, applicable the *anticipatory* or *pre-emptive* right of self-defence. Also, whether it is possible to resort to *preventive* self-defence against a future cyber-attack. Finally, in which situations can a State use the right of self-defence *a posteriori* against a cyber-attack.

C. **Methodology**

Once pinpointed the target of the research, it is mandatory to follow a cloning methodology approach. On one hand, it is necessary to point out that in general terms for the research process an interdisciplinary vision is always enriching. However, this interdisciplinary

treatment must not be to the detriment of the legal perspective in which the present investigation is being framed. The interdisciplinary perspective will contribute to a better understanding of the principles, rules and guidelines analyzed, since the other disciplines give additional support in a collateral sense to the legal approach. Thus, we are going to follow an interdisciplinary approach, but giving priority to the legal perspective, particularly of the Public International Law.

On the other hand, the issues raised by ICT, especially by Computer Network Operations (CNO), can only be embroidered through a holistic conception. Together with the domestic rules and strategies, it is necessary to take into account legal parameters, such as the regulation adopted by the EU or the Council of Europe, the guidelines with strong political connotations given by the UN, the ITU, the OSCE, the OCDE or the NATO, and the principles of sovereign equality, good faith or the prohibition of the threat or the use of force in international relations.

Nevertheless, we must consider the economic, socio-political and strategic factors that reveal the background of the contradictions between the developed States, more vulnerable to the CNO, and the developing States in respect to such operations. It should be emphasized that the possibilities offered by new ICT in order to satisfy the numerous shortcomings observed in international society are not negligible.

Due to the enormous difficulty of harmonizing the different conflicting interests and, consequently, finding suitable and viable solutions, at times, we only aim to developing a general conceptualization or a presentation of possible alternatives of a purely indicative character.

Starting from an interdisciplinary heuristic approach, it is convenient, in the first place, to fulfil an analysis of the main problems raised through cyber space, insofar as it is necessary; and, in the second place, to understand and delimit the legal issues that as a consequence of the implantation of the ICT, they are posed to Public International Law. Once the most significant ones have been detected from the point of view of State sovereignty, a study of the current state of each of these is then carried out, that is, the

degree of existing normativization is ascertained, with special emphasis on the main trends in the evolution of the States, as well as of their domestic law and, in general, the international practice, the international jurisprudence and the doctrine.

In any case, it should be noted that the main source of information lies in the State practice and in the positions expressed by governments in different international forums. In this sense, the documents of the UN, the ITU, the OSCE, the NATO, the EU or the Council of Europe will have a priceless value when providing possible indicators of an *opinio iuris*.

The multiplicity and heterogeneity of the legal instruments applicable and the great dispersion in its origin, together with the low degree of institutionalization, has led to the following an essentially inductive process at the moment of determining the relevant legal rules in each of the different issues to be regulated.

The difficulties existing in reaching solutions capable of responding to the aspirations of each of the States are evident. Given that it would be excessively ambitious to try to focus on the position of each State, it will provide a wide and panoramic view of the positions of the States, although always keeping in mind the most significant countries and international organizations.

Therefore, the starting point is not a previous conception that tries to corroborate itself, but the challenge consists in the elaboration -or at least that is intended- of a set of conclusions, induced from international practice, that synthesize and allow to obtain a coherent explanation of the factual components and of the legal magma, in such a way that enables to pronounce yourself on the existence and the scope of each of the legal rules examined.

In addition, this thesis is not limited to verifying the *lex lata*, but also analyses judgments which expressed what International Law must be international, including *lege ferenda* proposals. These are aimed at ensuring that the right of self-defence of the States can be predicated on both the formal and the substantial aspects. In other words, an international

legal framework capable of guaranteeing that ICT contributes to maintaining international peace and security with the ultimate aim of contributing to the progress of all peoples.

D**. Structure of the investigation**

From a first glance, the thesis has three chapters. Its first and second chapters provide the framework to developing the third chapter. In other words, firstly we will focus on the principle of the prohibition the threat or the use of force (first chapter) and, in the second chapter, we will stress one of the exceptions to such principle: the right of self-defence.

Therefore, in the first chapter, we will examine the principle of the prohibition of threat or the use of force in contemporary International Law. To clarify the scope of the principle better, the threat will be analyzed separately from the prohibition of the use of force.

In relation to the use of force, we describe the historical process of the formation and the development of the prohibition of the use of force by inquiring significant International Law instruments and international jurisprudence.

The identification of the scope and meaning of such prohibition is another part of our study. Here, on one hand, we will clarify that the prohibition applies only in *inter-State* relations and is not applicable in *intra-State* conflicts, except for situations where such conflicts become *internationalized.* On the other hand, the prohibition follows a non-restrictive approach since it works in any case of use of force, and not only when the territorial integrity or the political independence is violated.

Later on, we will study the *modalities* of the use of force. In this regard, we will distinguish the different forms of *armed force*, stressing the aggression (the most grave form), from other potential forms of use of force that may fall under the prohibition (political, diplomatic or economic coercion).

Finally, in this chapter will study the scope of the threat of force, which, after establishing the distinction between lawful and unlawful threat of force, we will analyze the restrictive approach to the threat of force under International Law.

The second chapter is related to the right of self-defence as an exception to the prohibition of the threat or use of force. First and foremost, we will analyze the characteristics of the right of self-defence and the role of the UNSC, and, secondly, the different requirements for the exercise of such right. In this regard, on one hand, it will be examined when does, according article 51 of the UN Charter, an armed attack carried out by State or non-State actors exist, and other issues such as the accumulation of events theory. On the other hand, other essential requirements established by general International Law (necessity, proportionality and immediacy) to justify the right of self-defence will be studied afterwards. In this sense, in relation to the immediacy requirement, we will attempt to clarify some legal controversies on the resort to preventive and anticipatory self-defence or even *a posteriori* in contemporary International Law.

The third chapter is the *hard core* of this research, appertain to cyber operations, in particular to the right of self-defence against cyber operation by States and non-State actors. In order to clarify the cyber operation, firstly we will highlight concepts, characteristics and classifications of such operations. Prior to start discussing whether a cyber-attack can constitute an *armed attack* or not, we will distinguish those kinds of cyber operations or related activities that can violate the principle of the prohibition of the threat or use of force from other cyber operations or activities below the level of such prohibition.

One of the most important sections of this chapter (and of the thesis), is related to those cyber operations that may justify the right of self-defence. In this sense, it will be analyzed whether a cyber-operation can constitute an armed attack and, if so, which kind of such operations can *amount to an armed attack* in the context of the right of self-defence. The fact that in the last decades most cyber operations were carried out by non-State actors has given rise to great challenges to the security of States. In this regard, the explanation of difficulties to provide clear evidence or attribute an armed attack to a State or a non-State actor is another relevant part of our research. Finally, the last section of this chapter is related to the adaptation of the other requirements of the right of self-defence (necessity, proportionality and immediacy) to the exercise of the right of self-defence against *cyber-*

attacks, with especial attention to the legal possibility to act in preventive or anticipatory self-defence before a cyber-attack occurs.

CHAPTER I

THE PRINCIPLE OF THE PROHIBITION OF THE THREAT OR THE USE OF FORCE IN INTERNATIONAL LAW

Historical development of article 2(4) of UN Charter is a key for a more precise comprehension of the principle of the prohibition of the use of force. The purpose of this chapter is to analyze the evolution of norms relating to the recourse to force. In this field, the first step is to undergoing surveys regarding the historical background on this article. In this sense, we must look at significant steps towards the banning of war in the 20th Century and then examine article 2(4), taking into account international organization acts, international jurisprudence or States practice, as significant instruments to elaborate the principle of the prohibition of the threat or use of force.

A. Development of the principle of the prohibition of the use of force

In the Classical International Law, the war was seen as a lawful mediator (*ius ad bellum* or the law on the use of force) to solve the controversies and never indicated when a war was lawful or not; the States determined when the cause of war was just and when it was not. In practice, the States resorted to war when their national interests required it. War was conceived as a self-help mechanism. However, during the wars the States had to respect the norms of *ius in bellum*[32] or the International Humanitarian Law (IHL).

1. *The first attempts to limit the war*

For a long time, the force has been one of the firm characteristics of the global system that has been used by humans for access their interests, which often resorted to violent means.

[32] *Ius ad bellum* relates more to the justice of a particular use of force *versus ius in bello* which relates to regulation use of force during armed conflict and to put limits on action during warfare; see KOLB, R.; HYDE. R., *An introduction to the International Law of armed conflicts*. Bloomsbury, 2008, p. 21.

In this context, Brownlie discussed how early civilizations such as India, China and Babylon ever resorted to war in that period[33].

Thus, war was a common feature for ancient societies from the middle era until modern era. *Just war* was a predominant doctrine that attempted to create restrictions on resort to war[34]. According to this view, two interconnected institutions (Pope and Holy Roman Emperor) were able to determine whether a particular war was just or not. Likewise, upon this doctrine, some theologians struggled to create some limitations to war, but war was essentially unrestricted and moral limitations were not successful in practice. According to the *just war* doctrine, a war is *just* if there is: i) a just cause (*justa causa*), such as war as a reaction in self-defence; ii) it is carried out by the lawful authority (*auctoritas publica*), the State as sovereign power has legitimate to make war; and iii) when the belligerent party had the right intention (*recta intentio*); which means just cause, correct intention and necessary measure[35].

Anyway, at the end of the 19th century, scholars and States made the first steps to changing the attitudes towards the unrestricted recourse to war[36]. In this field, The Hague Peace Conferences of 1899 and 1907 are the first majority diplomatic attempts to restrict warfare[37].

The Hague Peace Conferences somewhat attempted to limit freedom of war in International Law. In article 2 of The Hague Convention (I) of both 1899 and 1907 for the *Pacific Settlement of International Disputes*, contracting parties accepted that in a serious

---

[33] BROWNLIE, I., *International Law and the use of force by States*, Clarendon Press, 1963, p. 3-4.

[34] KOLB, R.; HYDE, R., *An introduction..., op. cit.,* p. 22.

[35] AREND, A. C.; BECK, R. J., *International Law and the use of force: beyond the UN Charter paradigm*, Routledge, 2013, p. 12-15.

[36] See HESELHAUS, S., "International Law and the use of force", in SCHWABACH, A., COCKFIELD, A. J. (eds.), *International Law and institutions*, Encyclopedia of Life Support Systems, 2009, p. 60-87, at p. 63.

[37] See SCHRIJVER, N., "The use of force under the UN Charter: restrictions and loopholes"*, Memorial lecture delivered at John W. Holmes.* Retrieved on 7 November, 2003, available at https://acuns.org/wp-content/uploads/2012/09/WebPageSchrijver_UseofForce.pdf**,**]visited on 21 June 2018[.

dispute, they would not recourse to armed force without having resorted to mediation of friendly States[38].

Regarding the First Hague Conference by attendance of twenty–six delegations, it seems that it took the initiative to pose a peace conference to reach objectives. The first step is to attempt to decrease military budgets through some agreed systems of disarmament while seeking to reduce the suffering of war, especially by members of the armed and naval forces. The second and parallel objective was to reinforce the systems available for the pacific settlement of international disputes, in particular through arbitration. The Conference was successful to its work on IHL and in the law on pacific settlement of disputes establishing the Permanent Court of Arbitration; however, it failed to decrease the military budgets and to plan for disarmament[39].

The Second Hague Conference struggled to impose limitations in the resort to war by the adoption of the *Convention II on the Limitation of the Employment of Force for the Recovery of Contract Debts*. In article 1, the members committed will not recourse to armed force for recovery of contract debts against other State, "however, [is] not applicable when the debtor State refuses or neglects to reply to an offer of arbitration, or, after accepting the offer, prevents any compromise from being agreed on, or, after the arbitration, fails to submit to the award". Likewise, article 1 of The Hague Convention (III) on the *Opening of Hostilities* established that Contracting parties "recognize that hostilities between themselves must not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an ultimatum with conditional declaration of war". As a result, Hague Conferences effectively represented a significant step to limiting the resort to war in international relations.

Consequently, these limitations on the resort to war agreed in a similar formal approach in the Bryan Treaties in 1913 between the United States and 22 countries, where a

[38] See DINSTEIN, Y., *War, aggression and self-defence*, CUP, 6th ed., 2017, p. 83.

[39] See BAETENS, F., "Hague Conferences (1899, 1907)", *Oxford Bibliographies online*, 2012, available at http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0115.xml, [visited on 24 June 2018].

suspension of the exercise of the right to start the war is prescribed. According to this approach, hostilities are authorized after recourse to International Investigation Commission and this must deliver its final report maximum within one year[40].

It is true that The Hague Conventions and Bryan Treaties represent important steps to restrict recourse to war because they entailed States to procedural obligations as regards to the beginning of war, but both were far from prohibiting war absolutely.

Until the establishment of The Covenant of the League of Nations in 1919, States and scholars struggled to develop a doctrine of less resort to war rather than prohibiting the recourse to war, strongly[41]. Hence, restrictions to initiate war were not enough to prevent the devastation of the World War I.

The Covenant of the League of Nations was the first attempt to create a collective security system to achieve international peace and security by giving preference to collective interests over national interests[42]. In this sense, Asrat claimed, "with the Covenant of League of Nations, the monolithic legal facade of international use of force was cracked"[43]. In fact, the Covenant was the first successful attempt to organize world order.

In this regard, the Covenant elaborated a formal approach to the restriction of resort to war[44]. In article 11, on one side, all States were obliged to avoid the war and, on the other side, the League was committed to take any action to keep peace among nations, as the idea of collective security suggests. Moreover, provisions under articles 12(1), 13(1) and 15(1) require all member States to submit to arbitration or judicial settlement or to enquiry by the Council of League of Nations, in any case that leads to conflict between members. Nevertheless, resorting to war is authorized after three months of the arbitral award,

[40] HESELHAUS, S., "International Law...", *op. cit*., p. 63.

[41] CARTER, B. E.; WEINER, A. S., *International Law*, 6th ed., Wolters Kluwer Law & Business, 2011, p. 935.

[42] McCOUBREY, H.; WHITE, N. D., *International Law and armed conflict*, Dartmouth, 1992, p. 20.

[43] ASRAT, B., *Prohibition of force under the UN Charter: a study of art. 2(4),* Iustus, 1991, p. 26.

[44] HESELHAUS, S., "International Law...", *op. cit*., p. 63.

judicial settlement or view of the Council. In other words, the Covenant established a *moratorium* on war.

Thus, the Covenant limited the resort to war, and prohibited it in the cases provided under article 10 where

> "The Members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the League. In case of any such aggression or in case of any threat or danger of such aggression the Council shall advise upon the means by which this obligation shall be fulfilled".

This obligation was ambiguous and, therefore, undermined its effectiveness[45] because the resort to war was forbidden loosely and not prohibited absolutely. For instance, after the invasion and the occupation of the Corfu by Italy in 1923, the Council of the League requested a Special Commission of Jurists, which struggled to clarify ambiguity of article 10. Such Commission expressed that not only war, but also other means of coercion, which are directly against territorial integrity and political independence of States, are not legally justified and violate article 10. Somehow, illegal war is not just aggression[46]. In sum, the Covenant is the first Treaty relating to the prohibition of war; it had a prominent role to restrict the resort to war, and also, it had the virtue to brake with the almost absolute permission of the use of force[47].

The member States of the Covenant attempted to elaborate a set of provisions by creating certain instruments to improve weak points of norms concerning the resort to the force. In this context, the *Geneva Protocol on the pacific settlement of international disputes* of 2nd October 1924, was accepted by the Assembly of the League. The main core of this Protocol was article 2, which stated that all contracting parties accepted the obligations that "in no case to resort to war either with one another or against a State which, if the occasion arises,

[45] McCOUBREY, H.; WHITE, N. D., *International law..., op. cit.*, p. 20-21.

[46] ASRAT, B., *Prohibition of force..., op. cit.*, p. 28.

[47] SCHRIJVER, N., "The use of force…, *op. cit.*

accepts all the obligations hereinafter set out, except in case of resistance to acts of aggression or when acting in agreement with the Council or the Assembly". Hence, this article is destined to abrogate the general right to wage war and sought to restrict circumstances to the use of force. Even though forty-eight States recommended approving this Protocol in the Assembly of the League, it failed to receive the necessary votes to enter into force and remained abortive until Kellogg-Briand Pact in 1928, when war became illegal[48].

As a result, the *Covenant of the League* in the same line with *The Hague Convention II on the Limitation of the Employment of Force for the Recovery of Contract Debts* against other State, set the peaceful settlement of dispute for decreasing the resort to war as a major priority and defined restrictions to recourse to force, but war was justified against States that did not accept arbitration decisions or Council reports[49].

2. *The prohibition of resort to war*

A watershed date in the history of regulation on the use of force is 1928, with the adoption of the *Kellogg Briand Pact*[50]. This is an instrument of national policy among 63 contracting parties, which was a record for that time. The Pact entered into force in 24th July 1929 and, for the first time, it had "the most decisive step towards the outlawing of recourse to war"[51]. In other words, we can envisage that it was the first widely accepted denunciation of war[52].

The Pact just comprises three articles. In article 1, contracting parties accepted "the condemn recourse to war for the solution of international controversies, and renounce it as

[48] DINSTEIN, Y., *War, aggression..., op. cit.,* p. 86.

[49] MILOJEVIC, M. B., "Prohibition of use of force and threats in international relations", *Teme,* 27(4), 2003, p. 609-637, at p. 587.

[50] The General Treaty for Renunciation of War (Kellogg-Briand Pact), 27 August 1928.

[51] ILC, "State responsibility", Documents of the thirty-second session, *Yearbook of ILC*, vol. II, part 1, 1980, p. 59, par. 100.

[52] SCHRIJVER, N., "The ban on the use of force in the UN Charter", in WELLER, M.; *et al.* (eds.), *The Oxford handbook of the use of force in International Law,* OUP, 2015, p. 465-487 at p. 468; see also HESELHAUS, S., "International Law...", *op. cit.*, p. 63.

an instrument of national policy in their relations with one another"; in article 2, they accepted that dealing with all disputes "shall never be sought except by pacific means"; and article 3 emphasized that the "Treaty shall be ratified by the High Contracting Parties named in the Preamble in accordance with their respective constitutional requirements, and shall take effect as between them as soon as all their several instruments of ratification shall have been deposited at Washington". In this context, some scholars claimed that the *Pact* caused International Law to progress from *ius ad bellum* to *ius contra bellum*[53] (the law on prevent war or limit the resort to use of force among States).

Thus, unlike the League Covenant that authorized resort to war in certain circumstances, the *Kellogg-Briand Pact* prohibited recourse to war entirely. In this regard, there was not any exception to the use of war in this general proscription. However, even if it was true that *Briand-Kellogg Pact* had a prominent role to developing the prohibition of recourse to war, it encompassed defects because it just outlawed war. In fact, the Pact did not include uses of force that do not constitute war. This defection facilitated the use of force, even military, in cases where there was no formal declaration of war; for instance, Japan's invasion of the Manchuria in the conflict of 1931[54]. Furthermore, by applying the phrase *national policy*, this led to misinterpret that the recourse to war in pursue of religious or ideological goals is lawful[55].

Consequently, *Kellogg-Briand Pact* represented an important step to developing the law in the field of the prohibition of the use of force and, unlike the Geneva Protocol; it entered into force and was widely regarded by States as authoritative[56].

---

[53] See HOWARD, M., "*Temperamenta belli:* can war be controlled?", in HOWARD, M. (ed.), *Restraints on war: studies in the limitation of armed conflict*, OUP, 1979, p. 23-35.

[54] SCHRIJVER, N., "The ban on the use of force…", *op. cit.*, p. 468; and DE MARCO, G.; BARTOLO, M., *A second generation United Nations: for peace and freedom in the 21st Century*, Routledge, 2009, p. 16.

[55] DINSTEIN, *War, aggression…, op. cit.,* p. 88.

[56] AREND, A. C.; BECK, R. J., *International Law..., op. cit.,* p. 23.

3. The prohibition of the use of force in the contemporary International Law

After World War II, in spring of 1945, the delegations of more than forty-nine States gathered in San Francisco to draft the UN Charter and finally adopted it on 26 June 1945. In its Preamble, all delegates pledged to "save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, and […] that armed force shall not be used, save in common interest […]"; therefore, it indicates that the UN Charter, by reliance to past procedures, attempted to open the new door to develop the prohibition of the use of force by replacing *war* by *armed force*. In other words, it struggled to expand the prohibition of the use of force[57]. In this regard, Higgins mentioned, "this prohibition is an improvement on earlier prohibitions such as those found in the Covenant of the League of Nations and the Kellogg-Briand Pact. It prohibits not only war, but also all use of force, falling short of war"[58].

Article 1(1) of the UN Charter holds that the main purpose or general objective of the organization is "to maintain peace and international security". The means to achieve this purpose are, on the one hand, the prohibition of *the threat or use of force* established in article 2(4) and, on the other hand, the *collective security system* "to take effective collective measures for the prevention and removal of threat to the peace, and for the suppression of acts of aggression or other breaches of peace".

The prohibition of the use of force expressed in article 2(4) is a fundamental principle[59] and the cornerstone[60] of the UN Charter. It mentions 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

[57] MILOJEVIC, M. B., "Prohibition of use of force...", *op. cit.*, p. 592; and BENNETT, T. W., "A linguistic perspective of the definition of the aggression", *GYIL*, 31, 1988, p. 48-69, at p. 67.

[58] HIGGINS, N., *Regulating the use of force in wars of national liberation: the need for a new regime: a study of the South Moluccas and Aceh*, Brill, 2010, p. 41.

[59] ICJ, *Military and paramilitary activities in and against Nicaragua* (Nicaragua *v.* United States of America*)*, judgment of 27 June 1986, *ICJ Reports* 1986, par. 188.

[60] ICJ, *Case concerning armed activities on the territory of the Congo* (Democratic Republic of Congo *v.* Uganda), judgment of 19 December 2005, *ICJ Reports 2005*, par. 148.

State, or in any other manner inconsistent with the purposes of the United Nations".

This article was adopted to cover up the previous weaknesses and to prevent violence in international relations. Actually, the drafters of the UN Charter endeavored to remove distinctions between war and other acts of force caused out of the abuse by some States to justify their use of force against other State such as the invasion of Italy to Corfu in 1923. Thus, article 2(4) goes farther of the reference to the war on previous instruments. The formula of the UN Charter is more complete than the prohibition contained in the Kellogg-Briand Pact. Firstly, it does not refer exclusively to war, but in a more generic way to the *use of force*; and secondly, it bans the *threat* of use of force[61]. Moreover, some short of war such as peacetime reprisal is prohibited under article 2(4).

Under article 2(4) the threat and the use of force is forbidden, and, alternatively, the Charter establishes the obligation of behavior to solve international disputes through peaceful means provided in article 2(3) and the *collective security system* in Chapter VII; in this regard, the UNSC has been equipped with the necessary powers to enforce the obligation of States to not resort to force, and has the faculties to decide coercive measures against States that do not observe such obligation.

After the establishment of the UN Charter, international community attempted to adjust article 2(4) in response to new circumstances. This adjustment has to be made by accommodative interpretation. This type of interpretation would be justified by different factors that make the UN Charter a rare international instrument[62]. In fact, since the UN Charter was established, amendments are exceptionals[63], and the provisions in the field of prohibition of the use of force have remained permanent in the various resolutions that

[61] SCHRIJVER, N., "The ban...", *op. cit.*, p. 470-473.

[62] ASRAT, B., *Prohibition of force..., op. cit.*, p. 59-60.

[63] For example articles 23, 27 and 61 had been amended according to UNGA, Resolution 1991 (XVIII) A and B, of 17 December 1963, which increased the Security Council members from 11 to 15, and the requirement of affirmative votes in the Security Council from 7 to 9.

have developed a set of rules to cope with a great variety of levels and type of force of article 2(4).

In this regard, the UNGA Resolution 2625 (XXV), in the same terms of the UN Charter, mentions that "Every State has a duty to refrain in its international relations from the threat or use of force against territorial integrity or political independence of any State, or in any State, or other manner inconsistent with the purposes of the United Nations". Nevertheless, it adds up several complementary rules; for instance “States have a duty to refrain from acts of reprisal involving the use of force”, to “organizing or encouraging the organization of irregular forces or armed bands including mercenaries, for incursion into the territory of another State”, and “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”. Moreover, “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"[64]. Thus, this resolution develops and extends the principle of the prohibition of the use of force.

Likewise, the UNGA Resolution 3314 (XXIX) tried to develop the principle of the prohibition of the use of force by considering the aggression as “the most serious and dangerous form of illegal use of force, being fraught, in the conditions created by the existence of all types of weapons of mass destruction, with the possible threat of a world conflict and all its catastrophic consequences”[65]. According to this Resolution, the aggression can be direct or indirect, issue that will be explained *infra.*

[64] UNGA, Resolution 2625 (XXV) “Declaration on Principles of International Law concerning friendly relations and cooperation among States in accordance with the Charter of the United Nations”, 24 October 1970, par.12 of the principle of the prohibition of the use of the force.

[65] UNGA, Resolution 3314 (XXIX) “Definition of aggression”, 14 December 1974.

Moreover, the UNGA in Resolution 42/22 reaffirms the obligation of States to maintain international peace and security in conformity with the purposes of the UN. On the one hand, it affirms the universal feature of the principle and its obligatory nature for all States and, on the other hand, it emphasizes the prohibition of certain *indirect* or subtle uses of force, such as instigating, assisting, organizing and supporting paramilitary, terrorist or subversive acts directed against other States and any other threat against the personality of the State. The Resolution, also mentions that States have the duty to refrain in international relations from military, political or any other form of coercion aimed against political independence and territorial integrity of States, and shall fulfil in good faith all its obligations in International Law[66]. In fact, this is a Resolution to condemn Gaddafi's regime for its support to international terrorism.

Also, the ICJ has had an important role in the development of the prohibition of the use of force. For instance, in the *Nicaragua case*, it states that "the principles as to the use of force incorporated in the United Nations Charter correspond, in essentials, to those found in customary international law"[67]. Furthermore, we must consider, along with other factors, that the rules declared by the Resolution 2625 (XXV) are the manifestation of an *opinio iuris* of the international community referring to the obligation to refrain from resorting to the threat or the use of force in international relations, and by themselves may "be regarded as a principle of customary International Law"[68].

The same opinion asserted in the *Israel Wall* advisory opinion[69]. Likewise, it is necessary to point out that in the *Legality of Nuclear Weapons,* the ICJ affirmed that "A threat or use of

[66] UNGA, Resolution 42/22 "Declaration on the enhancement of the effectiveness of the principle of refraining from the threat or use of force in international relations", 18 November 1987.

[67] ICJ, *Nicaragua case, op. cit*., par. 188.

[68] *Ibid.*

[69] ICJ, *Legal consequences of the construction of a Wall in the occupied Palestinian territory,* advisory opinion, of 9 July 2004, *ICJ Reports 2004*, par. 87.

force by means of nuclear weapons that is contrary to article 2, paragraph 4, of the United Nations Charter and that failed to meet all the requirements of article 51, is unlawful"[70].

Thus, these resolutions, along with the ICJ jurisprudence, have always had effects on the non-use of force in different ways. On one side, leading to strengthen the prohibition of the use of force and, on the other side, by extending the scope of the prohibition; for instance, covering the indirect use of force[71].

B. Scope and meaning of the principle of the prohibition of the use of force

We have to underline that the vast majority of authorities do not only support that the principle of the prohibition of the use of force is part of the customary International Law, but also "its status as a *ius cogens* norm"[72], and that its "categorization as a *ius cogens* norm is clearly an important development respecting the contemporary normative force of article 2(4)"[73]. However, to our understanding, it is difficult to advocate that all the prohibitions of the use of force that fall under article 2(4) achieve peremptory status, since only the most grave forms of the use of force, it means the aggression, have a *ius cogens* character[74].

---

[70] ICJ, *Legality of the threat or use of nuclear weapons,* advisory opinion, of 8 July 1996, *ICJ Reports 1996*, par. 105 c.

[71] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", in SIMMA, B., *et al*. (ed.), *The Charter of the United Nations. A Commentary,* vol. 1, 3rd ed., OUP, 2012, p. 200-234, at p. 25.

[72] ICJ*, Nicaragua case, op. cit*., separate opinion of judge Singh, p. 153; and *the Wall, op. cit*., separate opinion of judge Elaraby, p. 254; see also ILC, "Draft articles on the law of treaties", *Yearbook of the ILC*, 1966, vol. II, article 50, commentary 1; O'CONNEL, M. E., "*Jus cogens* , International Law higher ethical norms", in CHILDRESS, D. E. (ed.), *The role of ethic in International Law*, CUP, 2011, p. 78-100, at p. 78, and RANDELZHOFER, A.; DÖRR, O., "Article 2(4)" , *op. cit*., p. 231.

[73] O'CONNEL, M. E., "The prohibition of use of force", in WHITE, N. D.; HENDERSON, Ch. (eds.), *Research handbook on international conflict and security law*, Edward Elgar, 2013, p. 89-119, p. 113; see also RUYS, T., "The meaning of 'force' and the boundaries of the *jus ad bellum*: are 'minimal' use of force excluded from UN Charter article 2(4)?", *AJIL*, 108(2), 2014, p. 159-210, at p. 160.

[74] In this sense, according to the ILC "it is generally agreed that the prohibition of aggression is to be regarded as peremptory", ILC, "Draft articles on responsibility of States for internationally wrongful acts, with commentaries", *Yearbook of ILC*, vol. II, part 2, 2001, p. 112; see also, GREEN, J. A., "Questioning the peremptory Status of the prohibition of the use of force." *MJIL,* 32(2), 2011, p. 215-257, at p. 217; and CERVELL, M. J., *La legítima defensa en el Derecho Internacional contemporáneo*, Tirant lo Blanch, 2017, p. 21-22.

Also, before coping with the scope of the meaning of the principle of the prohibition on the threat or use of force, we have to point out that such principle only applies to cases where there is *no armed conflict*, such as acts of retaliation that imply the use of force, or to organize irregular forces to make raids in the territory of other States.

Finally, it is necessary to notice that the principle of the prohibition on the threat or use of force in the UN Charter and in the UNGA resolutions refers to individual States and to "groups of States" which is explicitly mentioned in the UNGA Resolution 2131 (XX)[75], and by the ICJ in the *Nicaragua case*[76].

1. *The prohibition only applies in "international relations"*

The principle of the prohibition of the use of force in the UN Charter is a response to the World War II, and it directly applies to inter-State conflicts[77]. This approach is obviously in view of the drafters of the UN Charter, particularly in article 2(4) as it is clearly manifested in the phrase *international relations.*

This conception has also been followed in the UNGA resolutions. In fact, since the establishment of the UN, the UNGA attempted to clarify the provisions relating to the principle of the prohibition of the use of force. The UNGA Resolution 2625 (XXV) reproduces such principle almost in identical terms; that it only applies to *international relations*. Moreover, it insists that "Every State has the duty to refrain from the threat or use of force to violate the existing international boundaries of another State […]", and "to refrain from organizing or encouraging the organization of irregular forces or armed bands including mercenaries, for incursion into the territory of another State"[78]. In addition, the Resolution 3314 (XXIX), in the definition of aggression under article 3 it continuously

[75] UNGA, Resolution 2131 (XX) "Declaration on the inadmissibility of intervention in the domestic affairs of States and the protection of their independence and sovereignty", 21 December 1965.

[76] ICJ, *Nicaragua case, op. cit*., par. 205; see also HENKIN, L., "The reports of the death of article 2(4) are greatly exaggerated", *AJIL*, 65(3), 1971, p. 544-548, p. 544.

[77] GRAY, C., *International law and the use of force*, 4th ed., OUP, 2018, p. 10; and RUYS, T., "The meaning of 'force'...", *op. cit*., p. 163.

[78] UNGA, Resolution 2625 (XXV), pars. 4 and 8 of the principle of the prohibition of the use of the force.

refers to the use of force in *the territory of another State;* it means that it is clearly limited to one State against another[79]. Likewise, in the Resolution 42/22, Declaration on non-use of force in international relations[80]. Thus, according to the UN Charter and these resolutions, the principle of the prohibition of use of force only refers to the inter-State relations[81].

Also, the ICJ in its advisory opinion on Kosovo affirms that "the principle of territorial integrity is an important part of the international legal order and is enshrined in the Charter of the United Nations, in particular in article 2, paragraph 4", and emphasized that the "scope of the principle of territorial integrity is confined to the sphere of relations between States"[82]. Then, non-State actors do not fall under article 2(4) of the UN Charter when they get financial or military assistance of another State[83]. Therefore, according to ICJ view, any act of violence by a non-State actor, if attributed to a State, would give rise to the right of self-defence[84].

However, the principle of the prohibition of the use of force only applies to *international relations* and does not prohibit the use of force at an internal level (it means within its borders against its own citizens or foreigner residents in its territory), it does not mean that no other rules of *ius cogens* can be violated when the force is used at a domestic level; for instance, committing an international crime such as the case of Saddam Hussein against the Kurds in 1991; the regime of Omar Al-Bashir in the Darfur conflict since 2003; Muammar Al-Gaddafi in 2011 or Bashar Al-Assad in 2012-2018.

---

[79] See UK, Doc. A/AC.134/SR.73, 6 August 1970 in UN, Doc. A/AC.134/SR.67-78, p. 93; Italy, Doc. A/AC.134/SR.73, 6 August 1970 in UN, Doc. A/AC.134/SR.67-78, p. 94; and Australia Doc. A/AC.134/SR.73, 6 August 1970 in UN, Doc. A/AC.134/SR.67-78, p. 95.

[80] See *Report of the Special Committee on Enhancing the Effectiveness of the Principle of Non-Use of Force in International relation meeting*, UNGA, 41 session, supp no 41 (A/41/41), of 13 March 1986, par. 67.

[81] GRAY, C., *International Law…*, *op. cit,* p. 40-43.

[82] *Accordance with International Law of the unilateral declaration of independence in respect of Kosovo*, advisory opinion, 22 July 2010, *ICJ Report* 2010, par. 80.

[83] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 213-214.

[84] ICJ, *Nicaragua case*, *op. cit*., par. 195.

a) Comparison between simple police measures and unlawful international measures

The principle of the prohibition of the use of force is applicable when one State uses the force against another State; for instance, when the entire air force squadron of one State crosses the border of another State constitutes *per se* an invasion and a violation of the prohibition of the use of force, even if no fire is opened[85]. This is different from simple police measures adopted where the State exercises its competences (on land, at sea or in the air) against individuals inside or outside its territories that break its laws; this cannot be defined within the scope of the prohibition of the use of force[86]. For example, military acts by territorial States to protect its own territory against intruding people, ships, air craft or the inspection or arrest of vessels that broke the law of a coastal State[87] or preventing or shooting an aircraft which unduly enters another State's airspace[88]. However, any forcible attack by a State against another State's ships or aircrafts of military or commercial nature, on or over the *high sea,* are acts of force and are "inconsistent with the purposes of the UN", and fall under the principle of the prohibition of the use of force[89].

One example of practice that confirms that some coercive acts by one State in territory of another State not violate the principle of the prohibition of use of force can be found in 1986, when Swiss police pursued offenders into French territory and opened fire to them;

[85] DINSTEIN, Y., War, aggression…, *op. cit*., p. 213; and RUYS, T., "The meaning of 'force'...", *op. cit*., p. 171.

[86] BOWETT, D. W., *Self-defense in International Law*, Praeger, 1958, p. 38; CORTEN, *O., The law against war: the prohibition on use of force in contemporary international law,* Hart, 2010, p. 52-54; RUYS, T., "The meaning of 'force'...", *op. cit*., p. 180; and RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 215

[87] See for instance, article 73(1) of the United Nations Convention on the law of sea, 10 December 1982.

[88] One emblematic example in this respect are the reactions to tragedy of the KAL flight 007 on 1 September 1983 where such Korean aircraft entered illegally in Soviet Union airspace and was shot down by fighters that apparently thought it was a spy plane, resulting deaths of the 269 passenger and crew; in the UNSC debates non of States invoked article 2(4) of the UN Charter; see DINSTEIN, Y., *War, aggression*…, *op. cit.*, p. 214; CORTEN, *O., The law against war..., op. cit.,* p. 52-66; and RUYS, T., "The meaning of 'force'...", *op. cit*., p. 173.

[89] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 215.

no one thought that this "right of pursuit", exercised without any legal basis, was a violation of the principle of the prohibition of the use of force[90].

To add, on 9 March 1995 the Canadian navy vessels arrested a Spanish fishing vessel on the high seas in accordance to their *Canadian Act* under the accusation of the infringement of the prohibition to fish standing stock. Spanish fishing vessel were released a few days later without any casualties, but Spanish officers on 28 March 1995 claimed it as a violation of the prohibition of the use of force of minimum level and criticized Canadian behavior. In response, Canada argued that they were applying simple conservation and management measures under national regulations. Eventually, the ICJ did not find any jurisdiction in this case and declared that "Boarding, inspection, arrest and minimum use of force for those purposes are contained within the concept of enforcement of conservation and management measures according to a 'natural and reasonable' interpretation of this concept"[91].

Regarding to the International Law of the Sea that authorizes the implementation of enforcement measures against foreign State vessels, policy measures by a State against individuals are not acts of force by one State against another[92]. Thus, the minimum use of force by States as management measures under national regulation against individuals whether it is inside or outside its territory, cannot violate the principle of the prohibition of the use of force and can well be defined as enforcement measures of territorial or extraterritorial scope.

[90] CORTEN, O., *The law against war…, op. cit.*, p. 54.

[91] ICJ, *Fisheries Jurisdiction case (*Spain *v.* Canada*),* judgment of 4 December 1998, *ICJ Reports* 1998, pars. 19 and 84.

[92] CORTEN, O., *The law against war…*, *op. cit.*, p. 55- 56.

b) Inapplicability of the prohibition of the use of force in the military intervention by consent

The prohibition of the use of force is applicable in *international relations* but it does not work in all circumstances that international border is crossed[93]. The expression intervention by valid consent applies to the presence of foreign troops in an internal conflict of another State to repress rebels in domestic conflicts[94]. The consent can be expressly and sometime upon previous agreement among States.

In this context, consent precludes wrongfulness of military intervention in other State. Thus, under International Law, external military intervention by invitation is lawful, except in position that its objective is to settle a civil war in favor of an established government[95].

Likewise, the International Law Commission (ILC) in article 20 of its *Draft articles on Responsibility of States* establishes that "Valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act in relation to the former State to the extent that the act remains within the limits of that consent"[96]. This means that actions committed by another State with consent are legal, but such acts have to be limited as far as the consent given**.**

Nowadays, the appearance of transnational non-State actors and the increasing number of internal conflict accompanied by violence, has caused that less international communities have a substantial interest in challenging the consent-exception *per se*[97]. In this sense, international communities accept justification of armed intervention in other States and

[93] *Ibid*, p. 149; see also NOLTE, G., "Intervention by invitation", in *Max Planck Encyclopedia of Public International Law*, 2010, available at http://opil.ouplaw.com, [visited on 2 July 2017].

[94] O'CONNELL, M. E.; EL MOLLA, R., "The prohibition on the use of force for arms control: the case of Iran nuclear program", *Penn State Journal of Law* & *International Affairs*, 2(2), 2013, p. 315-328, at p. 316.

[95] GRAY, C., *International law …, op. cit.,* p. 108.

[96] ILC, "Draft articles on responsibility...", *op. cit.,* vol. II, part 2, 2001.

[97] LIEBLICH, E., *International Law and civil wars: intervention and consent*, Routledge, 2013, p. 3.

International Law has never denied this legitimacy[98]. Then, this approach has been adopted by International Law when consent is given validly.

In this regard, it is only valid the consent given by effective authorities of the host State that are legally authorized to give such consent, and any intervention must be done after such permission[99]. During the Cold War, US and USSR frequently resorted to this legal factor by alleging an invitation of the Government or authorities of another State to justify their military interventions, such as the US in Dominican Republic (1965), in Panama (1989), etc., or USSR in former Czechoslovakia (1968) or in Afghanistan (1979).

In the case of Syria, since September 2014 some military interventions by US-led international coalition against the *Daesh* were carried out without any letter of consent[100]. In fact, achieving the consent has the key role to legitimate military intervention in the territory of another State. In this sense, Russia and Iran asserted that they have been fighting alongside the troops of Syria President Bashar Al-Assad against the rebel groups with valid consent[101].

Consequently, the provision of the prohibition of the use of force is not applicable in cases where the government of one State gives consent to another State to military intervention in their territory.

---

[98] See ICJ, *Armed activities on the territory of the Congo*, *op. cit*., pars. 51 and 52

[99] COUZIGOU, I., "The fight against the 'Islamic State' in Syria: towards the modification of the right to self-defence?", *Geopolitics, History, and International Relations,* 9(2), 2017, p. 80-106, at p. 82.

[100] "Identical letters dated 21 September 2015 from the Permanent Representative of the Syrian Arab Republic to the United Nations addressed to the Secretary-General and the President of the Security Council", see UNGA, Doc. A/70/385 and UNSC, Doc. S/2015/727, 22 September 2015.

[101] "Foreign intervention in the Syrian civil war under the scope of International Law", 23 May 2016, available at https://medium.com/@THE_CEO/foreign-intervention-in-the-syrian-civil-war-under-the-scope-of-international-law-b076d4f504, [visited on 2 July 2017].

c) *The prohibition applies in internationalized intra-State conflicts*

As it has been mentioned, the principle of the prohibition of the use of force does not play in the internal affairs, but in some positions may domestic conflict be converted into international conflict, and then such principle is enforceable[102]. In accordance with this view, the principle of the prohibition of the use of force is applicable in an internationalized intra-State armed conflict[103]. In this regard, the most prominent example is the external interventions in non-international armed conflict by other States[104]. For instance, in the case of Syria, the domestic conflict began in March 2011 with the simultaneous uprisings in many Middle East countries. However, the Syrian government has primarily been engaged in a civil war with some rebel groups in the scope of internal conflict, since September 2014 the international interventions turned the internal conflict into an international conflict[105].

In fact, the legal military intervention by invitation of Syria's government to targeting the *Daesh* by Russia and Iran, autonomous military intervention by US-led international coalition[106], the occupation of some parts of Northern Syria by Turkey, eventually a US missile struck against a Syrian Air Force airfield in 2017[107] and, with support of the UK and

---

[102] KIRCHHOFF, L., *Constructive interventions: paradigms, process and practice of international mediation*, 3, Kluwer, 2008, p. 11.

[103] "the prohibited use of force extends for that matter not just to direct military action but also to military support for irregular forces engaged in the internal conflict", see CORTEN, O., *The law against..., op. cit*, p. 129.

[104] MARAUHN, Th.; NTOUBANDI, Z. F., "Armed conflict, non-international", in LACHENMANN, F.; WOLFRUM, R. (eds.), *The law armed conflict and the use of force. The Max Planck Encyclopedia of Public International Law,* 2, OUP, 2017, p. 58-70, at p. 69.

[105] RULAC, Syria, at http://www.rulac.org/browse/countries/syria#collapse1accord, [last visited 20 January 2018].

[106] UNSC, Doc. S/2015/719, "Identical letters dated 17 September 2015 from the Permanent Representative of the Syrian Arab Republic to the United Nations addressed to the Secretary-General and the President of the Security Council", 21 September 2015; see also BANNELIER, K., "Military interventions against ISIL in Iraq, Syria and Libya and the legal basis of consent, *Leiden Journal of International Law*, 29(3), 3 February 2016, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2772474, [visited on14 May 2018].

107 "Trump launches military strike against Syria", *CNN*, 7 April 2017, available at https://web.archive.org/web/20170407021906/http://edition.cnn.com/2017/04/06/politics/donald-trump-syria-military/index.html, [visited on 23 June 2018].

France in April 2018[108], changed domestic conflict into internationalized conflict. In this context, the International Committee of Red Cross (ICRC) spokeswoman, Iolanda Jaquemet, mentioned that "any military operation by a State on the territory of another State without the consent amount to an international armed conflict"[109].

Then, any activities of a foreign State based on "organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State"[110], or the assistance to rebels in form of provision of weapons, logistics or any other type of support and participating in civil strife may internationalize a domestic conflict. As the ICJ affirmed, all these kind of interventions in another State are "regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States"[111]. Moreover, it declared that

> "it may be considered to be agreed that 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'"[112].

---

[108] COOPER, H., *et al*., "U.S, Britain and France strike Syria over suspected chemical weapons attack", *The New York Times*, 13 April 2018, available at https://www.nytimes.com/2018/04/13/world/middleeast/trump-strikes-syria-attack.html, [visited on 25 June 2018].

[109] ICRC, spokeswoman Iolanda Jaquemet in interview with Reuters, available at http://www.sbs.com.au/news/article/2017/04/08/syria-now-international-armed-conflict [last visited 8 April 2017].

[110] UNGA, Resolution 2625 (XXV), *op. cit*, par. 8 of the principle of the prohibition of the use of force.

[111] ICJ, *Nicaragua case*, *op. cit*., par. 195; see GRAY, C., *International law and…, op. cit*., p. 108-112.

[112] ICJ, *ibid.*

The ICJ added that this description, contained in article 3(g) of UNGA Resolution 3314 (XXIX), on the definition of aggression, "may be taken to reflect customary International law"[113].

Thus, the notion of internationalized intra-State conflict refers to the direct and indirect use of force by one State to an internal conflict of another State. In fact, any intervention of a foreign State to support non-State actors in the territory of another State can turn the domestic conflict into an international conflict[114].

2. Inapplicability of the prohibition of the use of force in intra-State conflicts

As it was mentioned, the principle of the prohibition on *the threat or use of force* established in International Law applies only in *international relations* among States[115]. In other words, such principle is only applicable to inter-State relations and cannot initially regulate the use of force in the case of intervention of non-State actors[116].

The scope of the prohibition of the use of force includes all inter-State conflict with any scale, and civil wars are outside of this principle[117]. Likewise, applicability of such principle in inter-State conflicts, has been affirmed by the *travaux preparatoires*[118] and several UNGA Resolutions which never attempted to expand such principle neither to domestic conflict nor to non-State actors.

Traditionally, civil war was an internal matter of sovereign States. Then, it would be logical to conclude that International Law remained *neutral* in civil war. The civil war in scale of

[113] ICJ, *ibid.*

[114] VITE, S., "Typology of armed conflicts in International Humanitarian Law: legal concepts and actual situations", *International Review of the Red Cross,* 91(873), 2009, p. 69-94, at p. 86.

[115] CORTEN, O., *The law against war…*, *op. cit.*, p. 163.

[116] HIGGINS, N., *Regulating the use of force…,op. cit,* p. 51.

[117] GRAY, C., *International law …, op. cit.,* p. 10.

[118] UNCIO, *Documents of the United Nations Conference on International Organization,* The Dumbarton Oaks Proposal for the Establishment of a General International Organization, San Francisco 1945, vol. IV, p. 3.

internal conflict is a domestic matter and the State does not need to invoke an exception to the prohibition of the use of force to justify its coercive measures[119].

In accordance with the *Institut de Droit International* (IDI) the term civil war

> "shall apply to any armed conflict, not of an international character, which breaks out in the territory of a State and in which there is opposition between: a) the established government and one or more insurgent movements whose aim is to overthrow the government or the political, economic or social order of the State, or to achieve secession or self-government for any part of that State, or b) two or more groups which in the absence of any established government contend with one another for the control of the State"[120].

Thus, under International Law, the civil war is completely an internal matter which remains under the jurisdiction of the State's domestic law. However, the legal situation changes if rebels succeed in establishing a stabilized *de facto* regime[121].

Next, we will categorize different actors in intra-State conflicts; there, on one hand, we will examine the institutions of rebellion, insurgency and belligerency, and, on the other hand, the figure of National Liberation Movements (NLM).

a) *Rebellion, insurgency and belligerency*

In conformity with traditional International Law based on the rate of challenges and intensity, three categories of groups are recognized against sovereignty of States in civil war: rebellion, insurgency and belligerency[122].

---

[119] CORTEN, O., *The law against war..., op. cit*., p. 129.

[120] IDI, *The principle of non-intervention in civil wars*, 8th Commission, 1975, article 1(1), available at http://www.idi-iil.org/app/uploads/2017/06/1975_wies_03_en.pdf, [visited 20 June 2018].

[121] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 214.

[122] CULLEN, A., *The concept of non-international armed conflict in International Humanitarian Law*, CUP, 66, 2010, p. 8.

The concept of rebellion refers to a situation of short-lived insurrection against the authority of a State[123]. The status of rebellion was vague with minor conflict in civil war and suddenly had been suppressed[124]. In fact, rebellions are defined within domestic law under the scope of sovereignty of States and any assistance by third State to rebels is an unlawful intervention in another State's sovereignty[125]. This has been emphasized by some UNGA resolutions, such as Resolutions 2131 (XX) which prohibit the intervention in civil strife occurring in another State[126], and Resolution 2625 (XXV) that enshrines prohibition of use of force in civil war within other States[127].

Traditionally, International Law did not ban States from the use of force within their territory to repress rebel groups in civil conflicts. Therefore, in this context, the principle of "benevolent neutrality" prevails in favour of the States[128]. In other words, States have not been prohibited from using their monopoly of legitimate force to restore its constitutional order[129].

In this field, some international treaties have given the States responsibilities or duties to preserve its national unity and territorial integrity "by all legitimate means"[130]. Likewise, a positive obligation to recover control of a breakaway region has repeatedly been affirmed by the European Court of Human Rights, in the *IIascu case* where*,* regarding to a domestic

---

123 *Ibid.*

124 HIGGINS, N., *Regulating the use of force…, op. cit,* p. 25.

125 See DHOKALIA, R. P., "Civil wars and International Law", *Indian Journal of International Law,* 11, 1971, p. 219-224, at. p. 224.

126 UNGA, Resolution 2131 (XX), *op. cit*., par. 8.

127 UNGA, Resolution 2625 (XXV), *op. cit.,* pars. 8 and 9 of the principle of the prohibition of the use of the force.

128 CORTEN, O., *The law against..., op. cit*., p. 129 and 135.

129 TANCREDI, A., "Secession and use of force", in WALTER, C., *et al*. (eds.), *Self-determination and session in International Law*, OUP, 2014, p. 68-94, at p. 69.

130 Article 3(1) of The Additional Protocol (II) to the Geneva Conventions of 12 August 1949, 1977, and article 8 (3) of Rome Statute of the International Criminal Court (ICC), of 17 July 1998.

conflict in Moldova, it obligated its government to "re-establish control over Transnistria"[131].

As it was affirmed *supra,* the reference to "international relations" in article 2(4) of the UN Charter means that the prohibition of the use of force is only applicable between States and not in domestic conflicts. Hence, rebels in the territory of a State cannot resort to the prohibition of the use of force to repel a central government's offensive. International Law is "legally neutral" in relation to the use of force within States[132], but it does not mean that States can violate other rules such as the ones related to human rights. Thus, International Law is neither condemning nor justifying insurrection in civil conflicts. Therefore, the States are the ones that do have the right and the duty to restore order in their territories[133]. The same idea of the right of the State to take decisions in internal matters has been confirmed in the UN Charter, deduced from article 2(7) which provides that "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any State […]". It has also been confirmed by the ICJ in *Nicaragua case* that the principle of the prohibition of the use of force "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States"[134].

Noteworthy, the UNSC interventions in some civil conflicts are not a manifestation of the extension of the prohibition of the use of force within a State[135]. These condemnations by the UNSC were related to the protection of human rights rather than the use of force under

---

[131] ECHR, *Case of Ilaşcu and Others v. Moldova and Russia*, application No 48787/99, judgment of 8 July 2004, *Reports of Judgment and Decision*, VII, par. 340; see TANCREDI, A., "Secession and use of force", *op. cit*., p. 69-70.

[132] CORTEN, O., *The law against war…*, *op. cit*, p. 128; and NASU, H., *International law on peacekeeping: a study of article 40 of the UN Charter*, Brill, 2009, p. 140.

[133] Article 3(1) of Protocol II Additional, *op. cit*, relating to the protection of victims of Non-international Armed Conflict, of 8 June 1977.

[134] ICJ, *Nicaragua case, op. cit*., par. 205.

[135] For instance, UNSC, Resolution 1244 on the situation relating Kosovo, 10 June 1999; see CORTEN, O., *The law against war…*, *op. cit*., p. 133.

article 2(4) of the UN Charter[136]. However, they have been interpreted as resolutions towards preventing the threat and tension from expanding to an international level[137].

The insurgency is a more serious nature than rebellion[138] and traditional International Law does not have an explicit definition of insurgency[139]. According to Wilson, there seems to be a general agreement that recognition of insurgency implies that a factual relation or acknowledgement of the existence of an internal war. There are no requirements for the degree of intensity of violence, the extent of control over territory, the establishment of a quasi-governmental authority or the conduct of operations in accordance with any humanitarian principles which would indicate recognition of insurgency as appropriate[140]. Lauterpacht affirms that

> "any attempt to lay down the conditions of recognition of insurgency leads itself to misunderstanding. Recognition of insurgency creates a factual relation in the meaning that legal rights and duties as between insurgents and outside States exist only in so far as they are expressly conceded and agreed upon for reasons of convenience, humanity or economic interest"[141].

The indeterminate scope of insurgency allows for the concept's manipulation by States to wish to define their relationship with insurgents. Third States may recognize the existence of insurgency without explicitly declaring an allegiance or adopting a position of neutrality towards the conflict[142]. On this point, Falk has written that the recognition of insurgency,

---

[136] CORTEN, *ibid*.

[137] TOMUSCHAT, C., "Secession and self-defence", in KOHEN, M. G. (ed.), *Secession: International Law perspectives,* CUP, 2006, p. 23-45, at p. 43.

[138] HIGGINS, N., *Regulating the use of force…, op. cit,* p. 25.

[139] WILSON, R. R., "Recognition of insurgency and belligerency", *American Society of International Law Proceedings*, 31, 1937, p. 136-143.

[140] WILSON, H. A., *International Law*, *and the use of force by national liberation movements*, OUP, 1990. p. 24.

[141] LAUTERPACHT, H., *Recognition in International Law*, CUP, 3, 2012, p. 276-277.

[142] See CASTREN, E., *Civil war*, Suomalainen Tiedeakatemia, 1966, p. 46-47.

> "Serves as a partial internationalization of the conflict, without bringing the States of belligerency into being. This permits third States to participate in an international war without finding themselves 'at war', which would be the consequence of intervention on either side once the internal war had been identified as a State of belligerency"[143].

In fact, there are two schools of thoughts in relation to insurgency[144]. Some scholars such as Higgins and Greenspan bring it out of remit of domestic law and put it to forum of International Law[145], whilst some others do not confer any rights or duties to the group and claim that this kind of group can be defined within domestic law[146]. Therefore, contrary to rebellion in civil war, status of insurgency is a "quasi-International Law status"[147]

Even though there is not clear threshold to distinguish insurgents from rebels, it is clear that insurgency must have a minimum of organization[148] with certain characteristics such as the requirement of military force to exercise sufficient control over its territory[149].

The recognition of insurgency is a very rare occurrence, but there is general agreement that the right of insurgents is limited to the territorial boundaries of the State involved[150]. Moreover, insurgents are allowed to enter into general agreements and arrange for

---

[143] FALK, R. A., "Janus tormented: the International Law of internal war", in ROSENAU, J. N. (ed.), *International aspects of civil strife*, Princeton Legacy Library, 1964, p. 185-248, at p. 200.

[144] OPPENHEIM, L., *International Law. A Treatise.* vol I, *Peace*, 2nd ed., Longmans, Green, and Co.,1948, p. 248-253.

[145] HIGGINS, R., "International Law and civil conflict", in LUARD, E. (ed.), *The international regulation of civil wars*, Thames and Hudson, 1972, p. 160-186, at p. 170; and GREENSPAN, M., *The modern law of land warfare*, University of California Press, 1959, p. 620.

[146] GREENSPAN, *ibid*; MILLEN, R. A.; METZ, S., *Insurgency and counterinsurgency in the 21st Century: reconceptualising threat and response*, Diane, 2004, p. 12-24; see also CASSIMATIS, A. E., *et al*., "Arms, traffic in", in LACHENMANN, F.; WOLFRUM, R., (eds.), *The law of armed conflict and the use of force. The Max Planck Encyclopedia of Public International Law*, 2, OUP, 2017, p. 87-96, at p. 89.

[147] FALK, R. A., "Janus tormented...", *op. cit*., p. 199; see also MENON, P. K., *The law of recognition in International Law. Basic principles,* Edwin Mellen Press, 1994, p. 110 and 123.

[148] MENON, P. K., *The law of recognition..., op. cit.*, p. 110.

[149] HIGGINS, N., *Regulating the use of force…,op. cit.,* p. 26.

[150] WILSON, H. A., *International Law ...., op. cit*., p. 25.

humanitarian protection through the ICRC[151]; however, it is generally agreed that other belligerents' rights, such as the right to blockade, does not attach to insurgents[152].

Belligerent groups in civil war is the greatest organization with serious nature against sovereignty of State in status of statehood. According to contemporary International Law, the prohibition of the use of force of article 2(4) of the UN Charter is not applicable in civil war except for situations where the central government has lost its control over a territory (failed State), and belligerent movements have risen to status of statehood. In this situation, civil conflict can arise international conflict and, as a result, article 2(4) is applicable[153]. In fact, belligerent groups in civil war challenge the State's sovereignty that increases the extent of the conflict, being it greater than other conflicts of other groups, such as rebels and insurgents.

In this context, certain characteristics are necessary to recognize the status of belligerency. These are, if: i) the insurgent occupied certain part of a State's territory, ii) they established a government and recognized a right of inherent sovereignty on that part of the territory, and iii) they conducted the hostilities by organized troops kept under military discipline and acting in compliance with the law of armed conflict[154]. In fact, recognition of belligerency was originated in the beginning of 19th Century when the UK and the US governments both granted this status to Spanish colonies' rebels[155].

Although, there are some ambiguities around belligerency, it is obvious that recognition of belligerency gives them rights and duties in International Law the same as a State[156]. One of

---

[151] FALK, R. A., "Janus tormented...", *op. cit.*, p. 100.

[152] WILSON, H. A., *International Law..., op. cit.,* p. 24-25.

[153] CORTEN, O*., The law against…, op. cit.*, p. 129-131.

[154] SCHINDLER, D., *The different types of armed conflicts according to the Geneva Conventions and Protocols*, Martinus Nijhoff, 1979, p. 141; see also AZAROVA, V.; BLUM, I., "Belligerency", in LACHENMANN, F.; WOLFRUM, R. (eds.), *The law of armed conflict ..., op. cit.,* p. 111-116, at p. 111.

[155] MENON, P. K., *The law of recognition...*, *op. cit.*, p. 124.

[156] WILSON, H. A., *International Law...*, *op. cit.*, p. 24; CULLEN, A., *The concept of non-international…, op. cit.,* p. 14; GUPTA, R., "Recognition of insurgent and belligerent organisations in International Law", 2014, p. 7, available at https://ssrn.com/abstract=2457749, [visited on 4 June 2018].

the factors to recognize insurgents in the status of belligerent is when it recognized by 'third States'.[157].

However, the most significant recognition of belligerency is by the central government of the territory (parent State). Nevertheless, reluctant of States to recognize and lacks of special pattern for this recognition, leading, in many cases, belligerency not be recognized, even if *de facto* they have already reached a remarkable level of belligerency, such as the conflict between *Fuerzas Armadas Revolucionarias de Colombia* and the State of Colombia[158].

Noteworthy, conflicts with rebels, insurgents and belligerents are still considered, in principle, as domestic matters and International Law merely intervenes to protect human rights or to take on the role of the UNSC of maintaining international peace and security[159]; hence, such interventions cannot be reason to the reorganization of these groups[160].

b) *National Liberation Movements (NLM)*

According to article 2 of the UNGA Resolution 1514 (XV), "All people have the right to self-determination; by virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development"[161]. The UNGA Resolution 2625 (XXV) adds that "every State has the duty to respect this right in accordance with the provisions of the Charter"[162].

---

[157] AGRAWAL, A., "Laws governing insurgency and belligerency in International Law", 19 February 2017, available at http://youngarenalitigators.blogspot.com/2017/02/laws-governing-insurgency-and.html, [visited on 23 April 2018].

[158] GUPTA, R., "Recognition of insurgent and belligerent organisations...", *op. cit.*, p. 7.

[159] Among others, see UNSC Resolution 993 on extension of the mandate of the UN observer mission in Georgia and settlement of the conflict in Abkhazia", 12 May 1995, par 5; UNSC Resolution 1494 on the situation in Georgia, 30 July 2003, par. 13; UNSC Resolution 1524 on situation in Georgia, 30 January 2004, par. 13; and UNSC Resolution 1554 on situation in Georgia, 29 July 2004.

[160] CORTEN, O., *The law against war..., op. cit.*, p. 134-135.

[161] UNGA, Resolution 1514 (XV) "Declaration on the granting of independence to colonial countries and peoples",14 December 1960, par. 2.

[162] UNGA, Resolution 2625 (XXV), *op. cit.*, par. 1 on the principle of equal rights and self-determination of peoples; see also the UNGA Resolutions 1541 (XV) on "Principles which should guide Members in

Theoretically, according to International Law, all colonial people have the right of self-determination and this right can be exercised through the National Liberation Movements (NLM), whom considers the legitimate representative of people to claim this right.

In contrast to civil war where the principle of 'benevolent neutrality' prevails in favour of the State, self-determination is qualified by legitimacy bestowed on the people struggling for its independence[163]. Obviously, this legitimacy internationalizes domestic conflict between State and NLM by certain international instruments where colonial people are under foreign domination or any people subject to a racist regime[164].

The question is whether the UNGA Resolutions, expand the scope of article 2(4) of the UN Charter out of inter-State conflicts, or just the right of self-determination gives people legitimacy to struggle without extending the principle of the prohibition of the use of force.

In this context, there have been serious discussions among States, especially between Western States and groups of Socialist Countries that joined to Non-Aligned States during the Cold War. Socialist and Non-Aligned States supported the extension of the scope of the

---

determining whether or not an obligation exists to transmit the information called for under Article 73e of the Charter", 15 December 1960, principle VII; UNGA, Resolution 2131 (XX), *op. cit*., par. 3 or UNGA Resolution 2160 (XXI) on "Strict observance of the prohibition of the threat or use of force in international relations, and of the right of peoples to self-determination", 30 November 1966, par. 3; and the ICJ, advisory opinions on *Legal consequences for States of the continued presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (197*0), advisory opinion of 21 June 1971, *ICJ Reports* 1971, p. 31, 63 and 65; and on *Western Sahara*, advisory opinion of 16 October 1975, *ICJ Reports 1975*, pars. 54-56, where it indicates that the right to self-determination of peoples is a customarily established principle; among the prolific bibliography on the right of self-determination see GROS ESPIELL, H., *The right to self-determination: implementation of United Nations resolutions,* United Nations, 1980; TOMUSCHAT, CH,(ed.), *Modern law and self-determination*, Martinus Nijhoff, 16, 1993; NIRMAL, B. C., *The right to self-determination in International Law,* Deep and Deep, 1999; MCCORQUODALE, R., *Self-determination in International Law*, Ashgate, 2000; CRAWFORD, J., *The right of self-determination in International Law: its developments and future*, ALSTON, Ph. (ed.), 2001; RAIČ, D., *Statehood and the law of self-determination*, Martinus Nijhoff, 2002; and ROEPSTORFF, K., *The politics of self-determination. Beyond the colonization process*, Routledge, 2013.

[163] IDI, *The principle of Non-Intervention...*, *op. cit*., 1975, article 5*;* see also CORTEN, O., *The law against war…, op. cit*., p. 135-136.

[164] See UNGA, Resolution 1514 (XV) "Declaration on the granting of independence to colonial countries and peoples", 14 December 1960, UNGA, Resolution 1541 (XV), and UNGA, Resolution 2625 (XXV), *op. cit.*; in this regard, the principle of territorial integrity, "only serve, under very specific conditions, as a limitation of the right of people to self-determination" see ODENDAHL, K., "The scope of application of the principle of territorial integrity", *GJIL*, 53, 2010, p. 511-540, at p. 511.

application of article 2(4) over the intra-State conflict between State and NLM. This view has been refused by Western States, which resorted to the phrase of "international relations", and by reliance on the UNGA Resolution 3314 (XXIX), to the definition of aggression, asserted that the intention of the UN Charter drafters regarding the principle of the prohibition of the use of force was a strict view to limit this prohibition to State against other State. In this sense, both the UK and the US asserted that this legitimacy of the right of self-determination for NLM is an advancement of the right of people and it does not relate to the prohibition of the use of force[165]. Hence, the NLM cannot fall within the legal framework of the principle of the prohibition of the use of force[166].

There is not any consensus among States in this issue. Seemingly, the recognition of the right of self-determination cannot expand the scope of the prohibition of the use of force over the intra-State conflict between a State and an NLM; this right only gives people legitimacy to struggle for independence[167]. This approach is the prevailing view in the international community of States. Thus, in the lack of any general agreement, it can only be concluded that the inter-state character of the rule contained in article 2(4) should be maintained in inter-State relations, even if this requirement must be combined with the recognition of a right of the peoples to self-determination[168].

3. *Can States use force when it is not against the territorial integrity or the political independence?*

The use of force is a politically sensitive and legally undetermined subject. Hence, it is not surprising that in this context there are serious controversies among authorities. The prohibition of the use of force is logically linked to the notion of external sovereignty that,

[165] UK, UN, Doc. A/C.6/SR.1092, of 11 December 1968, par. 10; UN, Doc. A/AC.119/SR. 16, of 9 September 1964; UN., Doc. A/AC.125/SR.21, of 22 March 1966, par. 6; and US, UN, Doc. A/AC.134/SR.59, of 22 July 1970, and UN, Doc. A/AC.134/SR. p. 52-66.

[166] For example, UK, UN, Doc. A/C.6/SR.1163, of 29 November 1969, p. 354, par. 25; and Australia, UN, Doc. A/AC.119/SR,17, of 9 September 1964, p. 14; see also UNGA, Doc. A/8018, Report of Special Committee on Principles of International Law concerning Friendly relations and Cooperation among States, Official Records of the General Assembly, 25th Session, Supplement No. 18, 1 May 1970, p. 112, par. 228.

[167] CORTEN, O., *The law against war..., op. cit*., p. 135, 137.

[168] *Ibid*, p. 137.

on one side, aims at protecting the identity and the personality of every State and, on the other side, preserving "generations from the scourge of war"[169].

a) *Purposes of the prohibition of the use of force*

The UN Charter is the main source of principles in contemporary International Law for the regulation of the use of force in international relations, and article 2(4) expresses a *fundamental principle* in this field[170]. Article 2(4) of UN Charter affirms that States shall refrain "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". Then, as it is mentioned *supra,* "the principle of territorial integrity is an important part of the international legal order and is enshrined in the Charter of the United Nations, in particular in article 2, paragraph 4"[171].

Article 2(4) provides an important number of legal and technical issues. Firstly, it establishes a legal obligation to UN members and, according to article 2(6), also to non-member States. Secondly, it addresses two targets that are under protection against unlawful threat or use of force[172]. On the one hand, "the territorial integrity or political independence of any State" is a specific example of protection of *sovereign equality* of all States and, on the other hand, it prohibits the threat or use of force "in any other manner inconsistent with the purposes of the United Nations". However, these two groups of protected values equated in one provision do not have the same nature. The aim of the prohibition of the threat and the use of force in the first part of article 2(4), "territorial integrity and political independence of any State" clearly refers to an inter-State conflict, but there are ambiguities towards the second part related to "Purposes of the United

[169] The UN Charter, preamble, par. 1

[170] ICJ, *Nicaragua case, op. cit*., par. 188.

[171] ICJ, *Kosovo* , *op. cit*., par. 80.

[172] SAYAPIN, S., *The crime of aggression in International Criminal Law:* Historical Development, Comparative Analysis and Present State, Springer Science & Business Media, 2014, p. 207.

Nations" which are listed in article 1(1) of the UN Charter as "maintenance of peace and security in international relations".

i) Protection of sovereign equality of all States

The historical drafting of article 2(4) of the UN Charter indicates that States in the initial Draft in Dumbarton Oaks proposal only referred to the prohibition of the use of force in any manner inconsistent with the purposes of the Organization[173]. Eventually, article 2(4) included the territorial integrity and political independence, which broadened the protection against the use of force by most powerful States, no matter how much States are powerful[174]. Thus, the protection of the territory is an expression of the sovereign equality of all States. In this sense, the concept of "territorial integrity and political independence" was reaffirmed in many of the UN instruments like UNGA Resolutions 1514 (XV), 2131(XX), 2625 (XXV) and 3314 (XXIX).

In regards to the importance of sovereign equality of States, the UNGA Resolution 1514 (XV), affirms that "all States shall observe faithfully and strictly" the provision of the UN Charter "on the basis of equality, of non-interference in the internal affairs of all State, and respect for the sovereign rights of all peoples and their territorial integrity"[175]. Later, the UNGA Resolution 2131 (XX) recognized an inalienable right of States to "the exercise of their sovereignty and the integrity of their national territory"[176].

The UNGA Resolution 2625 (XXV) did not only reaffirm the prohibition of the use of force, but also stressed the principle of sovereign equality of all States enshrined in article 2(1) of the UN Charter. This resolution explicitly emphasizes the inviolability of territorial integrity and the political independence of States based on State sovereignty. In fact, in contrast with 19th Century doctrine, where the use of force was an inherent right of State's

[173] UNCIO, *Documents of the United Nations Conference on International Organization,* Dumbarton Oaks proposals comments and proposed amendments, San Francisco 1945, vol. III, 1.

[174] MARXSEN, C., "Territorial integrity in International Law–its concept and implications for Crimea", *Zeitschrift für Ausländisches* , 75 (1), 2015, p. 7-26, at p. 9.

[175] UNGA, Resolution 1514 (XV), *op. cit*., par. 7.

[176] UNGA Resolution 2131 (XX), *op. cit*., par. 3.

sovereignty, contemporary International Law claims that the prohibition of the use of force is included in the concept of State sovereignty. This shift in International Law refers to a close relation between the concept of State sovereignty and the conception of illegal intervention[177].

Thus, the UNGA Resolution 2625 (XXV), by referring to the duty of States not to intervene within domestic jurisdiction of other States is claiming that no State or group of States have the right to intervene directly or indirectly in external or internal affairs of other State, and it prohibits any economic or political measures against the State's sovereignty. In this context, States in this Resolution declared that any "assist, foment, finance, incite or tolerate subversive, terrorists or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State"[178], is prohibited.

Likewise, this approach is recalled and reaffirmed by the UNGA Resolution 3314 (XXIX), where in article 1 declares that "aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State".

Hence, the protection of the sovereign equality of States is a fundamental principle of International Law; therefore, to guarantee the sovereignty and legal personality of all States, States must respect to the territorial integrity and political independence of another State. In other words, all States must respect the principle of the prohibition of the threat or use of force.

ii) Maintenance of peace and security in international relations

The UN was established in after the devastations of the World War II with the mission to maintain international peace and security in international relations. For instance, the UN Charter, in article 1 paragraphs 1 and 2 or article 2 paragraph 3 and 4, does this mission by preventing conflict, suppressing the use of force, helping States to resolve international

[177] PLANT, R., "Rights, rules and world order", in DESAI, M.; REDFERN, P. (eds.), *Global governance: ethics and economics of the world order*, Pinter, 1995, p. 190-218, at p. 155.

[178] UNGA Resolution 2625 (XXV), *op. cit.*, par. 2 in relation to the principle of non-intervention.

disputes by peaceful means, promoting friendly relations among States, achieving international co-operation in solving international problems of any kind and promoting and encouraging respect for human rights.

In conformity with article 2(4) of the UN Charter, the principle of the prohibition of the use of force covers a wide prohibition on the use of force by a State outside its borders, which is inconsistent with the maintenance of international peace and security and with the promotion of friendly relations among nations[179]. Likewise, in this context, the UNGA Resolution 2625 (XXV) by reference to international disputes from one State against another, it requests States to refrain from any action which may aggravate the situation and endanger the maintenance of peace and security in international relations, which is against the purpose of the UN Charter.

According to article 24 of UN Charter, the UNSC has the primary responsibility to maintain international peace and security, but it is not an exclusive authority. Thus, the UNGA, under Resolution 377A (V) "Uniting for Peace"[180], can discuss and recommend on circumstances even though the UNSC is still debating them. For instance, in the Suez Channel crisis in 1956, the UNGA decided to send peacekeeping force to Egypt even though the UNSC was simultaneously discussing on the issue[181]. Also, the UNGA, regarding to the Israeli Wall, requested an Advisory Opinion from the ICJ in 2003[182].

Article 39 of the UN Charter establishes that such responsibility of the UNSC must be exercised to determine "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 article 41 and 42, to maintain or restore international peace and security". The main problem in this context is with the definition of the terms "threat to the peace, breach of the peace" and "act of aggression" in international relations.

---

[179] MACLEAN, R. M., (ed.), *Public International Law*, HLT, 1996, p. 286.

[180] UNGA, Resolution 377A (V) "Uniting for peace", 3 November 1950.

[181] UNGA, Resolution 1001 (ES-I) on Middle East, 7 November 1956.

[182] UNGA, Resolution A/RES/ES-10/14 on "Illegal Israeli actions in occupied East Jerusalem and the rest of the occupied Palestinian territory", 8 December 2003.

Regarding to article 39 of the UN Charter, prohibition of force in article 2(4) is not limited to the aggression and it includes other operations that lead to the threat and breach of peace. The UNSC attempted to interpret the term "peace" in a negative sense. Thus, according to the Presidential Statement, economic, social, humanitarian and ecological crises are a threat to peace in absence of war and military conflict among States, and the proliferation of all Weapons of Mass Destruction (WMD) can threaten or disrupt the maintenance of peace and security[183]. As a result, the mere lack of war or armed conflict among States, does not ensure international peace and security.

b) *The non-restrictive approach on the prohibition of the use of force*

The UN Charter prohibited the threat and use of force in international relations, but there is not a transparent definition of what constitutes force. As has been mentioned, the prohibition of the use of force is supported by International Law and the UNGA attempted to codify some actions that may represent a violation of such prohibition by adopting different instruments. In this context, the most significant resolutions are the Declaration on the essentials of peace[184], Declaration 2625 (XXV) on friendly relations, Resolution 3314 (XXIX) on the definition of aggression, and Declaration 42/22 on the enhancement of the effectiveness of the principle of refraining from the threat or use of force. All these resolutions represent an important contribution to identify Customary International Law on the prohibition of the use of force and non-intervention against other States.

In fact, regarding the intention of the UN Charter drafters, it is noticeable that article 2(4) attempted to cover most of the prohibitions of the use of force in order to prevent abuses of force by adding the phrase "[...] or in any manner inconsistent with the purpose of United Nations". Therefore, the drafters tried to cover any uses of force with "a residual 'catch-all' provisions"[185]. Subsequently, the Charter does not give any hint of the prerequisite of

[183] UNSC, Doc. S/23500 on the responsibility of the Security Council in the maintenance of international peace and security, 31 January 1992.

[184] UNGA, Resolution 4/290, "Essential of peace", 1 December 1949.

[185] LACHS, M., *The development and general trends of international law in our time*, Martinus Nijhoff, 1980, p. 162; and DINSTEIN, Y., *War, aggression... op. cit.*, p. 93.

certain level of armed force; thus, minor violation of boundaries is prohibited by the principle of the prohibition of use of force[186]. In this sense, *integrity* has to be read as *inviolability* that includes any kind of forcible trespassing[187].

Since the UN Charter was established, some States to following their national interests, by reliance to article 2(4), have attempted to restrict the prohibition of the use of force just in situations that affects the territorial integrity and political independence of States and even this approach were supported by some scholars[188]. For instance, an unacceptable restrictive definition of prohibition of use of force by States appears in the *Corfu Channel* case in *Operation Retail*[189]*,* when minesweeping of Royal Navy of UK was carried out in the territorial waters of Albania. According to the UK, its operation never violated article 2(4) of the UN Charter because such operation was not directed against the political independence and the territorial integrity of Albania. The ICJ did not accept the UK claim[190]. This ICJ view has been also supported in *Nicaragua case*[191], *Oil Platform case*[192] and *Armed activities on the territory of the Congo*[193], where rejected restrictive approach to the prohibition under article 2(4). However, it seems that in some cases the ICJ had neutral

[186] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit.*, p. 216.

[187] RONZITTI, N., *Rescuing nationals abroad through military coercion and intervention on grounds of humanity*, Martinus Nijhoff, 1985, p. 8.

[188] For example, in order to justify Israel's strike against the Iraqi nuclear reactor at Osirik in1981, D'Amato's asserted that "the Israeli attack did not compromise the territorial integrity or political independence of Iraq, nor was it inconsistent with the purposes of the UN", see D'Amato, A., "Israel's air strike upon the Iraqi nuclear reactor", *Journal of International Law*, 77, 1983, p. 584.

[189] For instance, UK justification to act *Operation Retail*, see ICJ, *Corfu Channel case (*United Kingdom *v.* Albania), judgment of 9 April 1949, *ICJ Reports 1949,* p. 33-34*;*

[190] ICJ, *ibid,* p. 35; see GORDON, E., "Article 2 (4) in historical context", *YJIL,* 10(4), 1984, p. 271-278, at p. 275; and RUYS, T., "The meaning of 'force'...", *op. cit.*, p. 166.

[191] ICJ, *Nicaragua case, op. cit.,* par. 195.

[192] ICJ, *Case concerning Oil Platforms* (Islamic Republic of Iran *v.* United States of America), Judgment of 6 November 2003, *ICJ Reports 2003*, par. 51.

[193] ICJ, *Armed activities on the territory of the Congo*, *op. cit.*, pars. 153, 164.

language and cautious approach[194], particularly when the Court did not expressly refer to article 2(4) of the UN Charter and just used the phrase "policy of force"[195].

Also, in the *Israel-Uganda* conflict in 1976 on *Entebbe* circumstance, Israel claimed that the use of force against Uganda was a contemporary rescue mission and was not directed against territorial integrity and political independence of Uganda[196].

The same position was supported in the *Israel-Tunis dispute* on April 1988 when Israeli army commando group secretly entered in a suburb of Tunis and executed a leading figure of Palestinian Liberation Organization (PLO) and returned to Israel without engaging in combat. This operation, which resulted in the attack to the sovereignty and territorial integrity of Tunis, was considered a violation of article 2(4) by the UNSC[197].

Moreover, in the *Guyana-Suriname* circumstance in 2007, when the patrol boats from Suriname entered and disputed in the maritime zone under licenses of Guyana and ordered an oil prig and drill ship. Guyana qualified Surinam operation as a threat to resort to force and as a violation of article 2(4). In contrast, Suriname claimed that the taken measure were "reasonable and proportionate law enforcement measures" by reliance to *Fisheries Jurisdiction case* between Spain and Canada. Guyana denied Suriname claims and considered this case as wholly irrelevant as a precedent and contended "that case concerned enforcement measures against fishing vessels on the high seas and not the use of force directly arising from a maritime dispute between two sovereign States"[198].

---

[194] GRAY, C., "The International Court of Justice and the use of force", in TAMS, C. J.; SLOAN, J., *The development of International Law by the International Court of Justice*, OUP, 2013, p. 237-262, at p. 240.

[195] ICJ, *Corfu Channel case, op. cit.,* p. 35

[196] UNSC 1942nd meeting, on the Entebbe, 13 July 1976, par. 103, where Israel claimed that "Article 2(4) of the UN Charter should be interpreted as prohibiting acts of force against the territorial integrity and political independence of nations, and not to prohibit a use of force which is limited in intentions and effect to the protection of a State's own integrity and its nationals' vital interest, when the machinery envisaged by the United Nations Charter is ineffective in the situation".

[197] UNSC, Resolution 611 on Middle East, 25 April 1988, Preamble.

[198] ARBITRAL TRIBUNAL, *Award in the arbitration regarding the delimitation of the maritime boundary between Guyana and Suriname*, award of 17 September 2007, *RIAA*, XXX, part I, par. 444.

Eventually, the Arbitral Tribunal Award recognized Suriname measure as a threat to the use of force rather than law enforcement activities[199].

This approach is also defended by many scholars that emphasized that article 2(4) must be interpreted widely[200]; it means that the prohibition embraces any case of threat or use of force at the international level. Not applying the Charter to situations of use of force from which the application of article 2(4) has not been excluded, would be contradictory with the progressive development of the International Law[201]. As Brownlie pointed out, the preparatory work of the Charter clearly indicates the intention to ensure that small States have maximum protection against the actions of the most powerful and, therefore, cannot understand the expression "against the territorial integrity or political independence of any State" as having a restrictive effect[202].

Therefore, the Charter is aimed at suppressing the use of force as a means of resolving any international conflict. As Piñol affirms, after 1945 all uses of armed force, although it seems like a minor action, are unlawful based on article 2(4)[203]. Even so, some authors support that any armed humanitarian intervention, in principle, would fall under the prohibition of

[199] ARBITRAL TRIBUNAL, *ibid,* par. 445, in this paragraph tribunal "accepts the argument that in International Law force may be used in law enforcement activities provided that such force is unavoidable, reasonable and necessary. However, in the circumstances of present case, this Tribunal of the view that the action mounted by Surinam, on 3 June 2000 seems more akin to a threat of military action rather than a mere law enforcement activities".

[200] Among others, CORTEN, *O., The law against war..., op. cit.,* p. 51-52; RUYS, T., "The meaning of 'force'...", *op. cit*., p. 164; DINSTEIN, Y., War, aggression..., *op. cit*., p. 93-94; and GRAY, C., *International law*..., *op. cit.,* p. 37-39.

[201] SORENSEN, M., *Manual of Public International Law*, Mac Millan, 1968, p. 55-87.

[202] BROWNLIE, I., *International law..., op. cit.,* p. 267.

[203] PIÑOL, J., *El principio de no intervención*, unpublished Ph. D. thesis, UAB, 1978, p. 109.

article 2(4)[204]. However, some doctrine claims that an action must come along with injury or damage to be defined as force according to article 2(4)[205].

Hence, the intention of the drafters of article 2(4), the UNGA Resolutions as evolutional processes of the prohibition of use of force and the jurisprudence view on some circumstances, implicitly supports the non-restrictive view on the prohibition of the use of force. Furthermore, the majority of the doctrine moves in similar approach[206]. Thus, the prohibition of the use of force in article 2(4) includes any kind of force, independently of whether it is against territorial integrity and political independence or it is not.

4. *Modalities of the use of force*

Article 2(4) of the UN Charter is in the center of serious debates on proper interpretations of the meaning of *force*. The prohibition of article 2(4) by use term *force*, in contrast to other treaties[207] which just used the term *war*, clearly shows that both war in classical sense and other inter-State force, are covered by such prohibition[208]. In fact, the drafters of the UN Charter preferred to apply the phrase *use of force* to cover all forcible measures as *short of war*, expression that includes quick actions that do not involve major commitment of force[209]. Although the expression *force* never came with the adjective *armed*, the phrase *armed force* came in other articles of the UN Charter such as articles 41 and 46. Consequently, it seems that at the beginning, the prevailing view of force was limited to

[204] See DUPUY, R. J., "Droit d'ingerence et assistance humanitaire", in Homage to professor M. DIEZ DE VELASCO, *Hacia un nuevo orden internacional y Europeo*, Tecnos, 1993, p. 273-279; and FRANCIONI, F., "Balancing the prohibition of force with the need to protect human right: a methodological approach", in CANNIZZARO, E.; PALCHETTI, P. (ed.), *Customary international law on the use of force. A methodological approach*, Martinus Nijhoff, 2005, p. 269-292.

[205] CORTEN, O., *The law against war*…, *op. cit*., p. 70-71.

[206] Among others, GORDON, E., "Article 2 (4) in historical context", *op. cit.,* p. 276; HENKIN, L., *International law: politics and values*, Dordrecht*,* 1995, p. 115-116; KRITSIOTIS, D., "When States use armed force", *Cambridge Studies in International Relations,* 96, 2004, p. 45-79, at p. 58-59; and DINSTEIN, Y., War, aggression..., *op. cit*., p. 93-94.

[207] For instance, the Covenant of the League of Nations.

[208] MILOJEVIC, M. B., "Prohibition of use of force...", *op. cit*., p. 592.

[209] AREND, A. C; BECK, R, J., *International Law..., op. cit.*, p. 17.

armed force[210], but nowadays the scope of the term *force* in article 2(4) must denote violence and it does not matter what specific means, kinetic or electronic, are used to bring it about[211]. Hence, there are different modalities of use of force.

According to the last phrase of article 2(4), the use of force is banned "[…] in any other manner inconsistent with the purposes of the United Nations", to "save succeeding generations from scourge the war" (Preamble of the UN Charter). In this sense, some commentators asserted that the world is facing changes of the nature of international conflict[212] with the emergence of new weapons with highly lethal that represent a great threat to the UN purposes. As a result, article 2(4) does not only cover the armed force, but also comprises physical force of a non-military nature[213].

[210] See BOWETT, D. W., *Self-defense..., op. cit.,* p. 148; KELSEN, H.; TUCKER, R. W., *Principles of International Law*, Holt, Rinehart & Winston, 1966, p. 86; GORDON, E., "Article 2 (4) in historical context", *op. cit*., p. 273; SINGH, J. N., *Use of force under International Law*, Harnam, 1984, p. 212; RÖLING, B. V. A., "The ban on the use of force and the UN Charter", in CASSESE, A. (ed.), *The current legal regulation of the use of force,* Martinus Nijhoff, 1986, p. 3-9, at p. 4; and RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 208.

[211] DINSTEIN, Y., *War, aggression..., op. cit*., p. 90.

[212] AREND, A. C; BECK, R, J., *International Law..., op. cit.*, p. 29-33.

[213] BROWNLIE, I., *International Law..., op. cit.,* p. 362-363 and 376-377; and KELSEN, H.; TUCKER, R. W., *Principles*…, *op. cit*., p. 86.

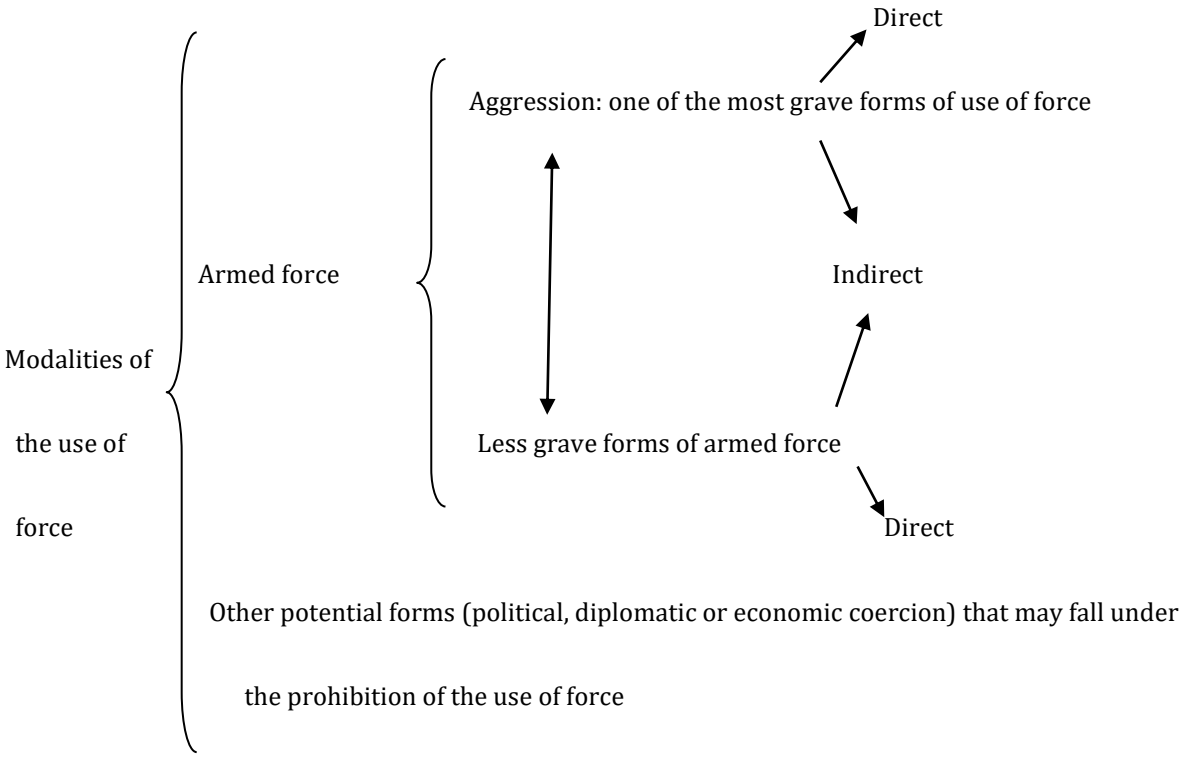

Figure 1. Modalities of the use of force

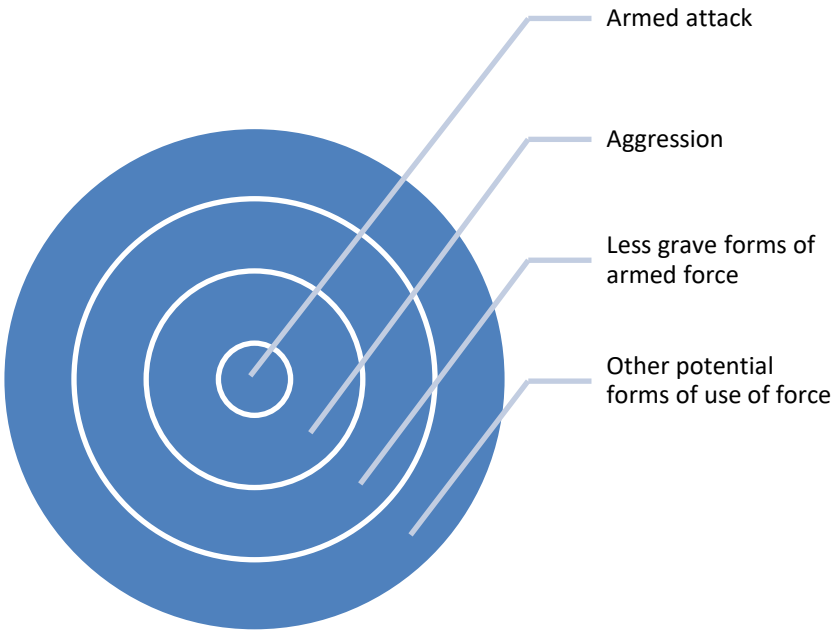

Figure 2. Hierarchy of the gravity of the use of force

a) *Armed force*

In the scope of the use of force, we have to distinguish between *the most grave forms of use of force* and *other less grave forms* of use of force[214]. The UNGA assimilates the most grave forms of use of force to the aggression which is defined in the Preamble of the Resolution 3314 (XXIX) as "the most serious and dangerous form of illegal use of force". The ILC adds that "under the heading of acts of aggression, the definition includes acts that do not necessarily all qualify as 'armed attacks'"[215]. Similarly, the ICJ affirms that *the most grave forms* of use of force can constitute an armed attack[216]. Some actions are below the

[214] ICJ, *Nicaragua case*, *op. cit.*, par. 191.

[215] ILC, "State responsibility", Documents of the thirty-second session, *Yearbook of ILC*, vol. II, part 1, 1980, p. 68, par. 117; see also KITTRICH, J., *The right of individual self-defence in Public International Law*, Logos Verlag, 2008, p. 32, where mentions "aggression is thus broader in scope than an armed attack and that only the most violate and gravest forms of aggression qualify as armed attack [...]".

[216] ICJ, *Nicaragua case*, *op. cit.*, par. 191.

threshold of aggression which expressed *less grave forms*[217] of use of force (see Figure 1) that also may breach the prohibition of the use of force, although they do not have *sufficient gravity* to constitute an aggression[218]. In this sense, undoubtedly article 2(4) of the UN Charter does not cover just armed attack as serious form of use of force[219], but also includes all military operations by one State directly or indirectly against another State.

i) Aggression: one of the most grave forms of the use of force

In fact, the *use of force* in article 2(4) of the UN Charter has relation with other provisions of the Charter that are in contra-peace situation in different terms as "aggression" in article 39 which has connection to the UNSC regarding "any threat to the peace, breach of the peace, or act of aggression", and in article 1(1), where it emphasizes to take collective measures to "the suppression of acts of aggression" to maintain international peace and security. However, the UN Charter does not define the term *aggression*. With the appearance of decolonization movements and cross border guerrilla invasions, interpretation of article 2(4) was unable to cover all kind of contemporary conflicts. Hence, the UN members attempted to develop the principle of the prohibition of the use of force by several UNGA Resolutions.

The different struggles to adopt a definition of aggression finally crystallized in article 1 of the Resolution 3314 (XXIX) which states that "aggression is the use of armed force by a State[220] against sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations".

Aggression can be *direct* or *indirect*. Following article 3 of the UNGA Resolution 3314 (XXIX), State may constitute a *direct aggression:* a) the invasion or attack by the forces of a State to the territory of another State (US invasion to Granada in 1983 or Israel invasion to

[217] REMIRO, A., *et al*., *Derecho Internacional*, Tirant lo Blanch, 2010, p. 668.

[218] UN Resolution 3314 (XXIX), *op. cit*., article 2.

[219] CORTEN, O., *The law against war*..., *op. cit.,* p. 52; in this context, Ruys asserts that there is a cascading relationship between force, aggression and armed attack, RUYS, T., "The meaning of 'force'...", *op. cit.*, p. 164.

[220] According to article 1 of Resolution 3314 (XXIX), the term State also includes a "group of States".

Lebanon in 2006), or any military occupation[221], even temporary (occupation of the Georgian cities by Russian forces in 2008)[222]; b) the bombardment by the armed forces of a State and the use of weapons against the territory of another State (bombardment of Libya by US in 1986); c) the blockage of ports or costs of a State by the armed forces of another State (Cuba crisis in 1962); d) the attack by the armed forces on the land, sea or air forces, or marine and air fleets of anther State (shod down Iran Air Flight by missile fired from US Navy in 1988); or e) the extension of the presence and activities of military force outside the existing commitment (presence of Ugandan troops in territory of DRC in 1998).

According the UNGA Resolutions 2625 (XXV)[223], 3314 (XXIX)[224], and 42/22[225], *indirect aggression* can be constituted[226] when a State allows its territory to be used by another State to carry out an act of aggression against a third State; the sending by a State, or on behalf of, armed bands, irregular or mercenary groups that carry out acts of armed force against another State with the same gravity as an aggression carried out by a regular force; or the support to acts of civil war or terrorism in other States or to consent activities organized in its own territory directed to the commission of these acts.

However, the Resolution 3314 (XXIX) in article 6 expressly states that it should not be interpreted in the sense that "in any way enlarging or diminishing the scope of the Charter", in fact, article 3(g) notes that acts such as "the sending by or on behalf of a State armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein" are classified as aggression; in other words, it includes the so-called *indirect aggression.*

---

[221] See also UNGA Resolutions 2625 (XXV), *op. cit.,* par. 10.

[222] See UNSC "The situation in Georgia", *Repertoire of the Practice of the Security Council, 2008-2009*, p. 132.

[223] UNGA Resolutions 2625 (XXV), *op. cit.,* par. 8 and 9 of the principle of the prohibition of the use of force.

[224] UNGA Resolution 3314 (XXIX), *op. cit.,* article 3, pars. g and f.

[225] UNGA, Resolution 42/22*, op. cit*., articles 4 and 6.

[226] Some authorities support that it would be more correct to talk of indirect of use of force; for instance CASANOVAS, O., "El principio de prohibición del uso de la fuerza", in DIEZ DE VELASCO, *Instituciones de derecho internacional* público, 18ª ed., Tecnos, 2013, p. 1074.

Moreover, the ICJ in the *Nicaragua case*, regarding the customary International Law, mentioned that an *armed attack* means "not merely action by regular armed forces across an international border" (direct aggression) but also the sending of armed bands, irregular or mercenary groups to the territory of another State (indirect aggression), as mentioned in article 3(g) of Resolution 3314 (XXIX)[227].

Therefore, armed attack as *the most grave use of force* locate in the form of aggression. applies to both regular and irregular uses of force. In these cases, to constitute an indirect aggression (armed attack), an incident should amount to the same gravity to an actual armed attack by regular armed forces and State should be substantially involved therein. Hence, in contrast to regular armed forces where the armed attack is established *per se,* an attack by irregular forces must have the same gravity of an armed attack by regular forces to constitute an aggression[228].

In accordance with the gravity (scale and effects), the sending of armed bands to the territory of another State with high gravity operation have been classified as an aggression rather than a less grave forms of use of force as *frontier incident* by regular armed force[229]. Thus, an armed attack, the most serious act of aggression[230], can also constitute an indirect aggression.

In addition, the ICJ pointed out that it is necessary to distinguish between "the most grave forms of the use of force (those constituting an armed attack) and other less grave forms"[231] (see Figure 2). In other words, according to the ICJ, when aggression constitutes

[227] ICJ, *Nicaragua case, op. cit*., par. 195.

[228] WEDGWOOD, R., "The ICJ Advisory Opinion on the Israeli security fence and the limits of self-defence", *AJIL,* 99(1), 2005, 52-62, at p. 52-57.

[229] *Ibid.*

[230] ILC view in article 33 mentioned that armed attack is "the most serious and unmistakable international offence of recourse to armed force in breach of the existing general prohibition of such recourse", see ILC, " Draft articles on State Responsibility", *Yearbook of ILC*, vol. II, part 1, 1980, p. 53-54, par. 88.

[231] ICJ, *Nicaragua case, op. cit.,* par. 191; and ICJ, *Oil Platforms case, op. cit*., par. 51.

an armed attack, this is the most grave form of the use of force and *frontier incidents* cannot necessarily be considered an armed attack regarding article 51 of the UN Charter[232].

In conformity with article 2 of the UNGA Resolution 3314 (XXIX) and the ICJ, the gravity is the only criteria to constitute aggression[233]. This position was also expressed by States during the *travaux* aiming at the definition of aggression, while the vast majority of States mentioned that only "the most serious uses of force are qualified as armed attack" regarding article 51[234]. In this line, Brownlie mentioned that a use of force must attain certain gravity to be defined as an armed attack under article 51[235]. Likewise, Gray claimed that the aim of the ICJ to distinguish between aggression (or an armed attack under article 51) and frontier incidents in paragraph 195 in the *Nicaragua case* has been summarized in degree rather than of kind[236].

Thus, the existence of an act of aggression (or armed attack, the most grave modality of aggression), it does not depend on the kind of weapons used (conventional weapons, WMD[237], drone attacks[238] or cyber-attacks), but rather on their degree of seriousness or graveness.

It is necessary to bear in mind that the UN Charter provisions are dynamic rather than fixed and can change through State practice[239]. Hence, there can be exceptions on extreme cases

---

[232] ICJ, *Nicaragua case, op. cit.,* par. 195;

[233] *Ibid*; see also O'CONNELL, M. E.; MIYAZMATOV, M., "What is aggression? Comparing the *jus ad bellum* and the ICC Statute", *Journal of International Criminal Justice,* 10(1), 2012, p. 189-207, at p. 191.

[234] RUYS, T., *'Armed Attack' and article 51 of the UN Charter: Evolutions in Customary Law and Practice*, CUP, 2010, p. 150.

[235] ICJ, *Oil Platforms case, op. cit*., par. 51; and BROWNLIE, I., *International Law..., op. cit.,* p. 366.

[236] GRAY, C., *International law…, op. cit.,* p. 154.

[237] The US military refers to WMD as chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.

[238] See BENJAMIN, M., *Las guerras de los drones. Matar por control remoto*, Anagrama, 2014; MONTOYA, R., *Drones. La muerte por control remoto*, Akal, 2014; and GÓMEZ, F., "Los ataques armados con drones en Derecho Internacional", *REDI*, 67(1), 2015, p. 61-92.

[239] GRAY, C., *International law …, op. cit*., p. 12; and GLASSMAN, A., "Evolution of the prohibition on the use of force and its conflict with human rights protection: balancing equally forceful *jus cogens* norms", *UCLA Journal International Law and Foreign Affairs,* 16, 2011, p. 345-384, p. 350.

when the use of non-military force may rise to the level of an armed attack under article 51[240]. According to Brownlie, the use of some non-conventional arms (for instance, biological and chemical weapons) can constitute use of force because these weapons are highly capable of destroying life and properties[241]. A non-armed attack under the same effects as an armed attack may well be considered among the most grave forms of use of force[242].

Both the *effects-based* and *means-based* standards are two parameters to read the article 2(4)[243]. *Effect-based* standard is focused on the level of harmful effects arising from an attack. From the perspective of the supporters of *effects-based*, *vague* was the intention of the drafters of article 2(4), because if they ever intended to restrict the scope of the prohibition of armed force, then they would have done so[244]. The *means-based* standard is upon base-instruments, which assumes that the use of force in article 2(4) just refers to the armed force.

According to deleterious *effect-based*, the use of biological and chemical weapons, the use of minor military and non–military physical force, such as intense cyber attacks, etc., can be included in the scope of the prohibition of the use of force, although upon *means-based* approach, economic coercions and cyber attacks has been excluded[245]. Some authors assert that the principle of the prohibition of the threat or use of force in the UN Charter does not

[240] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit.*, p. 210.

[241] BROWNLIE, I., *International law..., op. cit.,* p. 362.

[242] SCHMITT, M. N., "'Attack' as a term of art in International Law: the cyber operations context", *2012 4th International Conference on Cyber Conflict*, IEEE, 2012, p. 283-293, at p. 288.

[243] BOER, L. J., "'Echoes of times past': on the paradoxical nature of article 2 (4)", *JCSL,* 20(1) 2014, p. 5-26, at. p. 11.

[244] DELANIS, J. A.; KERSCHISCHING, G., quoted in BOER, L. J., "'Echoes of Times Past': On the Paradoxical nature of article 2 (4)", *JCSL,* 20(1), 2014, p. 11-12.

[245] BOER, L. J., "Echoes of time past'...", *op. cit.*, p. 10.

only cover the armed force[246], but also some conducts in large scale and directly against territorial integrity and political independence of another State[247].

Finally, it is worth mentioning that the acts listed in article 3 of the UNGA Resolution 3314 (XXIX) are not exhaustive (*numerus apertus)* and the UNSC may determine which other acts constitute the most serious and dangerous forms of illegal use of force with sufficient gravity to be considered as an aggression under the provisions of the UN Charter[248].

ii) Less grave forms of armed force

The principle of the prohibition of the threat or the use of force must be interpreted broadly. As it has been seen *supra*, according to the ICJ, in the scope of the use of force, it distinguished between *the most grave use of force* and *other less forms of use of force*. Then, some acts below the threshold of aggression in terminology of the Court expressed *less grave forms* [249].

In this context, the use of some conventional weapons, WMD, or cyber operations, are under the prohibition of the use of force, but, as it has been previously mentioned, whether they constitute an aggression or a use of less serious armed force, will depend on their degree of seriousness or graveness. In this regard, the ICJ explicitly did not draw the border between the most and less grave forms of force. However, in order to the comprehension of less gravity, the Court distinguishes *less grave forms of use of force* from a *mere frontier incident*[250]. In this regard, Dinstein affirms that if a rifle shot is fired by a soldier across the

[246] GOODRICH, L. Y., *et al*., *Charter of United Nations, Commentary and Documents*, Columbia University Press, 1969, p. 104.

[247] HIGGINS, R., *The development of International Law through the political organs of the United Nations*, Oxford, 1963, p. 177.

[248] O'CONNELL, M. E.; MIYAZMATOV, M., "What is aggression? Comparing the *Jus ad Bellum* and the ICC Statute", *Journal of International Criminal Justice,* 10(1), 2012, p. 189-207, at p. 194.

[249] REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 668.

[250] ICJ, *Nicaragua Case, op. cit*., pars. 191 and 195.

border of one State and the bullet hits a tree or a cow in another State, "no armed attack has been perpetrated since the episode falls below a *de minimis* threshold"[251].

Also, the less grave forms of armed force can be developed *directly* (mere frontier incident or threat of use of force) or *indirectly* (logistical support including provision of arms or other support to irregular armed force to another State). In relation to *direct* less grave forms of armed force, it can be assumed that mere frontier incident or the mere threat of use of force, is equaled a bothersome that does not have sufficient gravity (scale and effects) to constitute aggression (or an armed attack).

In this sense, the *Eritrea Ethiopia Claims Commission,* regarding Ethiopia's claim that justified the use of force with the right of self-defense, in article 11 declared that "localized border encounters between small infantry units, even those involving the loss of life, do not constitute an armed attack for the purpose of the Charter". In fact, the Commission, under article 12, stated that incidents with "geographically limited clashes between small Eritrean and Ethiopian patrols along a remote, unmarked and disputed border", are relatively minor to constitute an armed attack in sense of article 51[252]. However, logically every frontier incidents cannot be defined within less gravity when some of them are trivial and some are extremely grave[253].

Moreover, regarding the *indirect* less grave forms of armed force in the *Nicaragua case*, the ICJ by reference to the UNGA Resolution 3314 (XXIX), mentioned that the sending of irregular forces to the territory of another State to carry out acts of armed force must reach to amount of gravity as regular armed force[254]. Hence, acts of irregular armed forces less than sufficient gravity of regular armed forces cannot be defined as acts of aggression, but can be included in the scope of the use of force[255]. Then, the provision of weapons, logistical

[251] DINSTEIN, *War, aggression…*, *op. cit*. p. 210.

[252] ERITREA ETHIOPIA CLAIMS COMMISSION, partial award, *Jus Ad Bellum*, Ethiopia's Claims 1-8, (Ethiopia *v.* Eritrea), Award of 19 December 2005 *, RIAA*, XXVI.

[253] FITZMAURICE, G. G., "The definition of aggression", *ICLQ*, 1(1), 1952, p. 139.

[254] ICJ, *Nicaragua case*, *op. cit*., par. 195.

[255] See RUYS, T., "The meaning of 'force'...", *op. cit*., p. 164.

or any other support to irregular armed forces in another State are not defined as aggression. Therefore "Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States"[256].

Additionally, the Court stated that "the arming and training of the *contras* can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government", and "that the mere supply of funds to the *contras,* while undoubtedly an act of intervention in the internal affairs of Nicaragua […] does not in itself amount to a use of force"[257]. Then, supply of fund *per se* can not constitute the use of force and violate the principle of non-intervention.

Furthermore, it is necessary to ask whether it is legal to resort to the use of force against other acts that utilizes the force but are not materialized in an armed attack (article 51 of the UN Charter), when the international society is unable to stop and repress such acts. For instance, US military intervention in 1980 by means of a commando armed in the territory of Iran with the aim of releasing the members of the diplomatic and consular personnel retained as hostages. Although these interventions would be incompatible with the UNGA Resolution 2625 (XXV) "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"[258], some doctrine points out that they would not be prohibited by International Law[259].

However, the ICJ and other authors mention that the maintenance of peace must prevail over any other consideration[260] and "all use of force, except in the self-defence, is

[256] *Ibid.*

[257] *Ibid*, par. 228.

[258] UNGA, Resolution 2625 (XXV), *op. cit.*, par. 4 of the principle of the prohibition of the use of force.

[259] REMIRO, A., *et al*., *Derecho Internacional, op. cit.*, p. 686, and GUTIÉRREZ, C., *El estado de necesidad y el uso de la fuerza en Derecho Internacional*, Tecnos, 1987, p. 109-110.

[260] In this sense, the ICJ affirmed that "The primary place ascribed to international peace and security is natural, since the fulfillment of the other purposes will be dependent upon the attainment of that basic

incompatible with the fundamental purpose of the UN and, therefore, prohibited by article 2(4)"[261]. The ICJ did not clearly condemn the action of the US, but it was certainly not in favor of the justification of the use of armed force even in this extreme case, observing that "an operation undertaken in those circumstances, from whatever motive, is of a kind calculated to undermine respect for the judicial process in international relations"[262]. Therefore, this kind of intervention is not according to International Law, but the international community, due to the especial circumstances they are in, end up tolerating it.

b) *Political, diplomatic or economic coercions as potential forms that may fall under the prohibition of the use of force*

In the San Francisco Conference, the delegation of Brazil made the proposal that article 2(4) included the prohibition of economic coercion, but it was rejected[263]. Also, when the Preamble of the UN Charter mentions *force,* it connotes with the adjective *armed* ("armed force shall not be used, save in the common interest"). Likewise, when article 44 cites *force,* it refers to *military force* in a strict sense that obviously means armed force.

Afterwards, in the Special Committee that prepared the Resolution 2625 (XXV), the African, Asian, Latin American and Socialist delegations were in favour of including political and economic pressures in the concept of prohibition of the use of force, but Western delegations were objectively opposed[264]. Finally, these measures were included in the scope of the principle of non-intervention. Hence, coercion would be unlawful, not being

---

condition", ICJ, *Certain expenses of the United Nations*, (article 17, paragraph 2, of the Charter), advisory opinion of 20 of July 1962, *ICJ Reports 1962*, p. 168.

[261] JIMENEZ, E., *Derecho internacional contemporáneo*, Tecnos, 1980, p. 113, and PASTOR, J. A., *Curso de derecho Internacional Público y organizaciones internacionales*, 22ª ed., Tecnos, 2018*,* p. 662.

[262] ICJ, *Case concerning United States diplomatic and consular staff in Tehran*, *(*United States *v.* Iran), judgment of 24 May 1980, *ICJ Reports* 1980*,* par. 93.

[263] - UNCIO, *Documents of the United Nations Conference on International Organization*, Commission I, General Provisions, vol. VI, San Francisco 1945, p. 334.

[264] See PÉREZ, E., *Naciones Unidas y los principios de coexistencia pacífica*, Tecnos, 1973, p. 67; and DEMPSEY, P. S., "Economic aggression & (and) self-defense in International Law: the Arab Oil weapon and alternative American responses thereto", *Case Western Reserve Journal of International Law,* 9(2), 1977, p. 253-321, at p. 263-266.

based on the principle of the prohibition of the use of force but under the principle of non-intervention[265]. In this context, International Law Association (ILA) in its meeting in Johannesburg mentioned that "]economic[coercive measures *per se* are not equated with the type of force envisaged in article 2(4), although they may violate other prohibitions, such as the principle of non-intervention"[266]. In fact, the use of force is a form of intervention in the highest degree of graveness.

UNGA Resolution 3314 (XXIX) in article 2 consistently refers to the use of armed force and implicitly rejects the economic coercion as description of aggression; for instance, in the annex, aggression is defined as "the most serious and dangerous form of illegal use of force"[267], and article 3 constantly refers to the use of armed force; therefore, it implicitly rejects that economic coercion can be described as aggression[268].

Thus, San Francisco Conference and subsequently, when negotiating some general multilateral treaties[269]and debated UNGA resolutions of great relevance[270], the non-aligned and socialist States, whose objective was the total and unconditional prohibition of force, armed or otherwise, attempted to open extensive interpretations of the term "force" without success[271]. Therefore, all diplomatic, political or economic coercions are under the

[265] CARRILLO, J. A., *Soberanía del Estado y Derecho Internacional*, Tecnos, 1969, p. 222; LARAE- PÉREZ, C., "Economic sanctions as a use of force: revaluating the legality of sanctions from an effects-based perspective", *Boston University International Law Journal*, 20(1), 2002, p. 161-188, at p. 171; DINSTEIN, Y., *War, aggression…, op. cit*., p. 90; and AUST, A., *Modern treaty law and practice*, CUP, 2013, p. 256.

[266] ILA, *Draft Report on aggression and the use of force,* Committee on the Use of Force, Johannesburg Conference, 2016, p. 3, available at file:///C:/Users/hamed/Downloads/Draft%20Conference%20Report%20Johannesburg%202016.%20(4).pdf, [visited on 25 June 2018].

[267] *Cfr*. FARER, T. J., "Political and economic aggression in contemporary International Law", in CASSESE, A. (ed.), *The current regulation of the use of force,* Martinus Nijhoff, 1986, p. 121-132, at p. 126-127; and ALEXANDROV, S., *Self-defence against the use of force in International Law*, Kluwer, 1996, p. 113.

[268] DINSTEIN, *War, aggression*…, *op. cit*. p. 210, p. 90.

[269] For instance the Vienna Convention on the Law of Treaties.

[270] For example Resolutions 2625 (XXV) and 3314 (XXIX).

[271] REMIRO, A., *et al*., *Derecho Internacional, op. cit.,* p. 669.

principle of non-intervention[272]. As a result, implicitly over the years, the prevailing view on the meaning of force is limited to the *armed force*[273].

Moreover, the *Chatham House Principles* affirmed that "an armed attack involves the use of armed force and not mere economic damage"[274] and the ILA emphasized that "article 2(4) is generally accepted as referring to the use of 'armed' or 'physical' force"[275]. In this sense ILA mentioned that

> "even a wide interpretation of force under article 2(4) has its limits. Economic pressure, as noted earlier, is excluded from the notion of force in this context. The limitation to armed or physical force, however, faces certain challenges in light of recent and potential future developments, such as inter-state cyber operations"[276].

Remiro emphasizes that the problem of the scope of article 2(4) of the UN Charter is still alive and points out that Declaration 42/22 is ambiguous. While in the Annex, paragraph 18, it states "the duty of the States to refrain in their international relations from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of any State"[277], in the paragraph 1 it literally reaffirms article 2(4) of the UN Charter. Later, the *status quo* is consolidated in article 33(2.a) stating that nothing

---

[272] EGEDE, E.; STUTCH, P., *Politics of International Law and international justice*, Edinburgh University Press, 2013, p. 202; and RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit.*, p. 215; see also TRAPP, K. N., "Terrorism and the Internantional Law of State responsibility", in SAUL, B. (ed.), *Research handbook on International Law and terrorism*, Edward Elgar, 2014, p. 39-56, at p. 42.

[273] GOODRICH, L. M., *et al., Commentaire de la Charte des Nations Unies [signée le 26 juin 1945 à San-Francisco]*, La Baconnière, 1948, p. 115; see also, among others, JIMENEZ DE ARECHAGA, E., *Derecho constitucional de las Naciones Unidas*, Escuela de Funcionarios Internacionales, 1958, p. 84-85; PIÑOL, J., *El principio de no intervención…, op. cit.,* p. 107-111; RUYS, T., "The meaning of 'force'...", *op. cit.*, p. 163; PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 660-661, and CASANOVAS, O., RODRIGO, A., *Compendio de Derecho Internacional Público*, 7th., Tecnos, 2018, p. 420.

[274] The *Chatham House Principles of International Law on the use of force in self-defense*, 2005, published in *ICLQ*, 55(4), 2006, p. 963-972, p. 965.

[275] ILA, *Report on aggression and the use of force, op. cit.,* p. 2-3.

[276] *Ibid*, p. 3

[277] Moreover, article 8 of the Declaration 42/22 states that "No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind".

in the Declaration will be understood in such sense that "enlarging or diminishing in any way the scope of the provisions of the Charter concerning cases in which the use of force is lawful"[278].

However, part of the doctrine indicates that when political, economic, diplomatic or ideological pressures constitute a very serious coercion; that is "they make the normal life of a State impossible" and they address the violation of the territorial integrity or the political independence of a State, then article 2(4) may come into play[279].

Then, in principle politically, economically or diplomatically coercion does not fall under the prohibition of the threat or use of force, but in some especial circumstances we cannot exclude such possibility.

C. Scope of the prohibition of the threat of force

Prior to establish the UN Charter, article 10 of the League of Nations Covenant prescribes that "In case of […] any threat […] the Council shall advise upon the means by which this obligation shall be fulfilled".

Then, the Covenant forbids to States the threat of the aggression against territorial integrity or political independence of its members, and grant to the Council of the League of Nations the power to advise such members on the means that they should adopt in order to protect them in case of threat of aggression[280].

In the UN Charter, article 2(4) does not only prohibit the use of force, but also explicitly includes the prohibition of the threat of force. In fact, the *threat of force* was included as a contractual provision in the UN Charter to fill up shortage in the Covenant of the League of

[278] REMIRO, A., *et al*., *Derecho Internacional*, *op. cit.,* p. 669.

[279] HIGGINS, R., *The development..., op. cit.,* p. 177.

[280] TSAGOURIAS, N., "The prohibition of threats of force", in WHITE, N. D.; HENDERSON, Ch. (eds.), *Research handbook on international conflict and security law*, Edward Elgar, 2013, p. 67-88, at p. 68.

Nations[281]. However, article 2(4) does not make clear what kind of threats can violate the prohibition of threat of force in International Law. Recently scholars have developed many studies on the threat to peace within the meaning of article 39 of the UN Charter or to "threat" in scope of "preventive self-defence", but authors rarely have studied the threat of force according to the specific meaning of article 2(4). Hence, there is distinction between *threat of force* in article 2(4) and *threat of peace* in other articles of the UN Charter[282]. For instance, article 11(3) refers "to situations which are likely to endanger international peace and security", and articles 33(1), 34, 37(2) and 99 mention some disputes that "the continuance of which is likely to endanger the maintenance of international peace and security".

In this context, although some UNGA Resolutions, such as 2625 (XXV), 3314 (XXIX) and 42/22, reaffirmed the prohibition of the threat of force in International Law and reinforced such prohibition under article 2(4), none of them explicitly explained *which* and *when* the threat of force is unlawful or made clear the notion of threat of force. It seems that these Resolutions took a mission to clarify the definitions of the prohibition of threat of force[283], but unfortunately, they never put enough effort to draft the basis to develop the threat issue[284].

1. *Different approaches to the definition of the threat of force*

The UN Charter is a primary source of law, but to comprehend the scope of the threat of force, it is suitable to search other significant sources, such as the UN documents, the ICJ jurisprudence, the UN members practice or academic literature[285].

---

[281] STÜRCHLER, N., *The threat of force in International Law*, CUP, 53, 2007, p. 2.

[282] See SCHMITT, M. N., "Pre-emptive strategies in International Law", *MJIL,* 24(2), 2003, p. 513-548, at p. 530-531.

[283] GREEN, J. A.; GRIMAL, F., "The threat of force as an action in self-defence under International Law, *VJTL,* 44(2), 2011, p. 285-328, at p. 291.

[284] STÜRCHLER, N., *The threat of force*..., *op. cit.*, p. 3.

[285] *Ibid,* p. 4.

However, there are limitations to conceive the ICJ view in the field of the threat of force, because there are only a few decisions and they contain a superficial analysis[286]. Also, regarding the inbuilt fuzziness in language of the UN Charter towards the threat of force, neither its *travaux preparatoires* nor the UNGA made clear definitions of the threat. In this context, there have recently been scholar and governmental endeavours to minimize this ambiguity and clarify the meaning the threat in International Law, particularly in article 2(4).

According to the Random House Dictionary of the English Language, a threat is "a declaration of an intention or determination to inflict punishment, injury, death or less on someone in retaliation for, or conditionally upon, some action of course; an indication of probable evil, violence, or loss to come". Moreover, the Oxford Dictionary of Law defines a threat as "[...] the expression of an intention to harm someone with the object of forcing them to do something".

Another definition of threat was posed during the drafting of the UNGA Resolution 2625 (XXV) where Chile stated that "[…] the expression 'threat' of force shall refer to any action, direct or indirect, whatever the form it may take, which tends to produce in the other State a justified fear that it or the regional community of which it is a part will be exposed to serious and irreparable harm"[287].

In this field, one of the most important classical definitions of the threat of force is given by Brownlie that a threat of force "consists in an express or implied promise by a government of resort to force conditional on non-acceptance of certain demands of that government. If the promise is to resort to force in conditions in which no justification for the use of force exists, the threat itself illegal"[288]. This definition is confirmed and followed by recent

[286] See ICJ, *Legality of nuclear weapons, op. cit*., par. 47; and GREEN, J. A; GRIMAL, F., "The threat of force...", *op. cit*., p. 292.

[287] Chile, UN, Doc. A/AC.125/L.23, 24 March 1966, c, and A/AC/ 125/SR, 23 March 1966, par. 31.

[288] BROWNLIE, I., *International Law..., op. cit.,* p. 364;

literatures[289]. In this sense, Sandurska mentioned that "A threat is an act that is designed to create a psychological condition in the target of apprehension, anxiety and eventually fear, which will erode the target's resistance to change or will pressure it toward preserving the status quo" and "a threat of force is a message, explicit or implicit, formulated by a decision maker and directed to the target audience, indicating that force will be used if a rule or demand is not complied with"[290].

As we have seen, in the majority of definitions of the threat of force, a demand of a threatening actor is a fundamental issue. However, in view of some scholars, such demands are not a necessary requirement for the existence of the threat of the use of force in the sense of article 2(4)[291]. In this regard, Roscini states that "A threat of force under article 2(4) can be defined as an explicit or implicit promise of a future and unlawful use of armed force against one or more States, the realization of which depends on the threatener's will"[292]. Therefore, Roscini, by referring to the economic crisis in Taiwan after China's missile test on water near Taiwan Nuclear Power Plants in 1995, indicates that sometimes threat itself leads to damage even before the threatened target is materialized[293].

Also, according to Corten, the term threat of force "referred to an announcement of an act of violence for the purpose of intimidating a State to change its policies" and brings up "to any action, direct or indirect, whatever the forms may take, which tends to produce in the other State a justified fear that the regional community of which it is a part will be exposed to serious and irreparable harm"[294].

---

[289] GREEN, J. A.; GRIMAL, F., "The threat of force...", *op. cit*., p. 294; and LAUREN, P. G.,"Ultimata and coercive diplomacy", *International Studies Quarterly,* 16(2), 1972, p. 131-165, at p. 137.

[290] SADURSKA, R., "Threat of force", *AJIL,* 82(2), 1988, p. 239-268, at p. 241-242.

[291] DINSTEIN, Y., *War, aggression*..., *op. cit*., 2011, p. 92; WHITE, N. D.; CRYER, R., "Unilateral enforcement of Resolution 687: A threat too far?", *Cal. W. Int'l L.J.*, 29, 1999, p. 243-282, at p. 253-254; and ROSCINI, M., "Threats of armed force and contemporary International Law", *NILR,* 54(2), 2007, p. 229-277, at p. 235; See also ICJ, *Legality of nuclear weapons, op. cit*., oral proceedings, Indonesia remark CR/95/25, of 3 November 1995, p. 34; and Qatar CR/95/29, of 10 November 1995, p. 27.

[292] ROSCINI, M., "Threats of armed force…", *op. cit*., p. 235.

[293] *Ibid*., p. 236.

[294] CORTEN, O., *The law against war*…, *op. cit.,* p. 100.

The ILC held different meetings between 1981 and 1996 to investigate and prepare a explicit declaration on the threat of force. The consideration of the definition of the threat of aggression, given by the ILC can be valuable. Firstly, the ILC distinguished "threat of aggression" from "preparation of aggression". In the light of "threat of aggression", threat may occur in two ways: first, with sign or presage that may constitute danger and is source of fear[295]; and second, by gestures or acts that indicates the intention of a person to harm. In this sense, it mentioned that

> "The term threat […] does not result from a dispute or a situation which, in itself, constitutes a danger to peace [in the sense of article 33 and 34 of the UN Charter]. Rather it is the intention expressed or manifested by a State to commit an act of aggression. The concrete evidence of this intention is blackmail or intimidation, either oral or written. The threat may also consist of material deed: the concentration of troops near a State's borders, a mobilization effort widely publicized by the media, etc. It is in this second sense that the term is used in article 2, paragraph 4, of the Charter […]"[296].

But in "preparation of aggression", the Commission referred to "the preparation by the authorities of a State of the employment of armed force against another State for any purpose other than national or collective self-defence"[297]. As a result, the ILC members felt that it is difficult to differentiate between unlawful and lawful act based on this definition; besides, other members noticed fundamental defects in their notions[298].

Maybe due to this reason, in 1989 the ILC provided different definitions on the threat of aggression based on an enumerative approach. In its declaration, the word *threat* indicated

---

[295] "threat of force is kind of coercion that create a psychological condition of anxiety and fear", see SEELOS, B., *The Anti-secession law and the use of threat - is China`s policy towards Taiwan a violation of art 2 (4) UN Charter?,* Diplomarbeit, 2009, p. 31.

[296] ILC, "Draft code of offences against the peace and security of mankind", Document of the thirty-seventh session, *Yearbook of ILC,* vol. II, part 1, 1985, p. 73, par. 91

[297] *Ibid*, p. 73, par. 93.

[298] STÜRCHLER, N., *The threat of force…, op. cit.,* p. 4.

> "[…] acts undertaken in view to making a State believe that force will be used against it if certain demands are not met by that State, under the terms of the article, the threat of aggression may consist in *declarations*, that is to say expressions made public in writing or orally; *communication*, that is to say messages sent by the authorities of another government by no matter what means of transmission; and, finally, demonstration of force such as concentrations of troops near the frontier. This enumeration is indicative, as shown by the words 'or any other means'"[299].

Therefore, ILC based on an enumerative approach attempted to clarify that the threat of force ever can be constitute by communication (orally or writing) or by depict of force near frontier. Then, it is irrelevant how State transmit their threat to other State.

In 1991, versions of *the Draft Code of offences against peace and security mankind* referred to the threat of aggression as a separate and specific offence[300]. Article 16(2) of the 1991 *Draft* attempted to define the threat as "declaration, communication, and demonstration of force or any other measures which would give good reason to the government of a State to believe that aggression is being seriously contemplated against that State"[301]. However, this definition of threat of aggression was deleted in the definitive version of the *Draft Code* in 1996 transmitted to the UNGA, because some members felt that this approach to the threat was too ambiguous to entail individual criminal responsibility and just a few States included the preparation, planning and incitement of war of aggression in their criminal codes. In fact, States disagreed with the ILC view that threat of aggression had to be placed in a future criminal code[302]. Apparently, this view that threat of aggression had to be included in the definition of aggression under International Criminal Court (ICC) Statute was unresolved. Nevertheless, States were reluctant to include threat of aggression into a

[299] ILC, "Draft Code of crimes against the peace and security of mankind", Report of the Commission to the General Assembly on the work of its forty-first session, *Yearbook of ILC*, vol. II, part 2, 1989, p. 68.

[300] ILC, "Draft Code of crime against peace and security mankind", Summary records of the meeting of the forty-first session, *Yearbook of ILC, Yearbook*, vol. I, 1991, p. 203.

[301] *Ibid.*

[302] STÜRCHLER, N., *The threat of force…, op. cit.,* p. 32.

definition of aggression.[303]. In addition, the UNGA Resolution 56/152 of 19 December 2001 emphasized that the prohibition of threat of force stressed the obligation to refrain from the threat of force not only for UN members, but also for *all States*[304].

2. *Distinction between lawful and unlawful threats of force*

The prohibition of the threat of force in article 2(4) of the UN Charter does not mean that all threats of force are prohibited. In this direction, if the use of force is lawful, then the threat of force ought to be lawful. Also, if the use of force is unlawful, then, the threat would be illegal too.

a) *Unilateral and defensive lawful threat*

According to the prohibition of the threat and use of force in article 2(4) of the UN Charter and in the UNGA Resolutions such as 2625 (XXV) and 3314 (XXIX), threat and use of force are coupled and there is a direct link between threat and use of force in any circumstance. Hence, the threat of force could only be unlawful in circumstances where the use of force itself is illegal[305].

As it is mentioned *supra*, regarding the definition of threat of force, Brownlie was pioneer to illustrate such relationship by proposing that the threat and the use of force are directly related. Also, this approach is confirmed as authoritative reading of UN Charter text by other prominent scholars[306] and by the ICJ. The Court followed this view by rendering its

---

[303] ASSEMBLY OF STATES PARTIES (ICC), *Informal inter-Sessional meeting of the Special Working Group on the Crime of Aggression*, 5th Session, Doc. ICC-ASP/5/SWGCA/INF.1, of 5 September 2006, p. 9-10, and *Report of the Special Working Group on the Crime of Aggression*, 5th Session, Doc. ICC-ASP/5/SWGCA/1, 29 November 2006, p. 2; see also, ROSCINI, M., "Threats of force …, *op. cit*., p. 268.

[304] UNGA Resolution 56/152, 19 December 2001, par. 2.

[305] STÜRCHLER, N., *The threat of force…, op. cit.,* p. 38.

[306] WHITE, N. D.; CRYER, R., "Unilateral enforcement...", *op. cit*., p. 251-254; MYERS, M. A., "Deterrence and the threat of force ban: does the UN Charter prohibit some military exercises", *Military Law Review*, 162, 1999, 132-179, at p. 171; HSIAO, ANNE HSIU-AN., "Is China's policy to use force against Taiwan a violation of the principle of non-use of force under International Law?", New England Law Review*,* 32, 1998, p. 723; McCOUBREY, H., ;WHITE, N. D., *International law …, op. cit.,* 1992, p. 55-56; and ASRAT, B., *Prohibition of…, op. cit.,* p. 138-144.

opinion in the *Legality of nuclear weapon*s, where it linked legality of threat with legality of use of force, stating that

> "The notions of "threat" and "use" of force under article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal -for whatever reason- the threat to use such force will likewise be illegal. In short, if it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter. For the rest, no State-whether or not it defended the policy of deterrence -suggested to the Court that it would be lawful to threaten to use force if the use of force contemplated would be illegal"[307].

The Court statements were also supported by the Award of 2007 in the *Guyana–Suriname case*[308]. Moreover, several States have argued that the threat of force is prohibited under the same circumstances as the use of force, such as Iran[309], Czech Republic[310], Nauru[311], Malaysia[312], Mexico[313], Qatar[314], San Marino[315] and the US[316]. Furthermore, this point of view is supported by part of the doctrine[317].

---

[307] ICJ, *Legality of Nuclear Weapons*, *op. cit*., par. 47.

[308] ARBITRAL TRIBUNAL, Guyana *v.* Surinam, *op. cit*., par. 229-30.

[309] ICJ, *Legality of nuclear weapons, op. cit*., Verbatim Record, CR/95/26, 6 November 1995, p. 24.

[310] The Czech Republic "rejects the threat of force as an instrument of international policy", even if it is for a good purpose, UN, Doc. S/PV.3439, 17 October 1994, p. 11.

[311]ICJ, *Legality of nuclear weapons, op. cit;* according Nauru, the threat "is itself a kind of use", Memorial of the Government of Nauru, of 15 June 1995, p. 11, 23.

[312] *Ibid*, written statement of the Government of Malaysia, 19 June 1995, p. 8.

[313] *Ibid*, written statement by the Government of Mexico, 19 June 1995, p. 7.

[314] *Ibid*, Verbatim Record, CR 95/29, 10 November 1995, p. 27.

[315] *Ibid*, Verbatim Record, CR 95/31, 13 November 1995, p. 20.

[316] *Ibid*, Verbatim Record, CR 95/34, 15 November 1995, p. 79.

[317] GREEN, J. A; GRIMAL, F., "The threat of force...", *op. cit* , p. 292-295, where they mentioned "conceptual coupling for the prohibitions for threat and use of force"; and *Tallinn Manual 2.0*, *op. cit*., rule 70.

In this sense, in circumstances where the UNSC authorizes the use of force by States or international organizations, those threats are not against article 2(4)[318]. An example of unilateral lawful threat of force is related with the occupation of Kuwait by Iraq in 1990, where the US was clearly threatening by sending naval, air and land troops in the region against Iraq. US also formed a broad coalition and threatened to use the force if Iraq troops did not withdraw from Kuwait. In the same line, the US and the UK threatened to use the force against Iraq prior to the beginning of *Operation Iraqi Freedom* in 2003. These threats were lawful since they were authorized by the UNSC Resolutions of 678 (1990), 687 (1991) and 1441 (2002)[319]. On the contrary, the threats by the NATO on 13 October 1998 to air strike against Serbia if president Milosevic did not fulfill his obligations under the UNSC Resolutions are a clear example of an unlawful use of the threat of force, since its actions were not in compliance with the UNSC Resolutions[320].

Furthermore, there is legal uncertainty in the scope of self-defence. Several serious debates have taken place on the lawfulness of defensive threat of force. According to international jurisprudence, self-defence is lawful when the use of force (defined by scale and effect), occurs against an armed attack under article 51 of the UN Charter with consideration of the requirements of necessity and proportionality. A defensive threat of force is as a message or movement by a State against another State to repel an armed attack. In this context, the ICJ abstained from determining precisely whether answering to a threat by using the right of self-defence is lawful or not. According to a presumptive legality, a defensive threat is deemed lawful if the armed attack has enough scale and effects, but there seems to be certain ambiguities on the scale and effect of the armed attack.

---

[318] DINSTEIN, Y., *War, aggression.., op. cit.,* p. 92-93; see also UNSC Resolution 1154, 2 March 1998, and 1441, of 8 November 2002, where the Council threatened Iraq with 'serious' and 'severest' consequences if it not comply with previous resolutions.

[319] ROSCINI, M., "Threats of armed force...", *op. cit*., p. 237; however, in this issue some authors rejected that Security Council Resolutions has authorized military action against Iraq, see HMOUD, M., "The use of force against Iraq: occupation and Security Council Resolution 1483", *Cornell International Law Journal*, 36(3), p. 435-453, at p. 438.

[320] Among others, CHARNEY, J. I., "Anticipatory humanitarian intervention in Kosovo", *AJIL,* 93(4), 1999, p. 834-841, at p. 838; JOYNER, D. H., "The Kosovo intervention: legal analysis and a more persuasive paradigm", *EJIL,* 13(3), 2002, p. 597-619, at p. 618; and FRANCHINI, D.; TZANAKOPOULOS, A., "The Kosovo crisis-1999", in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 594-622, at p. 600-603.

Moreover, the legality of defensive threat of force is linked to the legality of anticipatory right of self-defence. The legality of defensive threat depends on the existence of an imminent armed attack, and the threat accomplishes the requirements of the right of self defence[321]. The *Caroline Case* in 1841 is a robust evidence of legal opinion and practice supporting anticipatory self-defence; that is a defensive threat. This approach is reaffirmed by the UN Report *More Secure World,* where anticipatory self-defence is permissible when the armed attack is imminent[322]. Given the lack of imminent threat or armed attack, States cannot take lawful defensive threat or use of force according to the right of self-defence and must render their evidence to the UNSC to get authorization to the use of force[323]. The Cuba Missile Crisis in 1962 is an appropriate example of this issue when in this circumstance, building a Nuclear Missile Bases in Cuba and breaking naval blockade by *USSR* ships, the US threatened to use the force[324]. In reaction to US threats, USSR asserted that building Missile Bases in Cuba is a right to make deterrent preparation against possible US invasions and this State is not entitle to intervene in Cuba's affairs[325]. However, while it is not clear if the US defensive threat was lawful, it can be useful as a way of an example to see how complex can sometimes be to realize if one's defensive threat is lawful or not.

Subsequently, the warning or threat to forcible defensive reaction by a victim State cannot breach article 2(4) of the UN Charter[326]. The precedents of this approach are revealed in *Falkland Island case* between the UK and Argentina, where the UK dispatched its military forces by threatening to remove Argentina force from Falkland Islands if they did not withdraw. Also, in the occupation of Kuwait in 1990, the US threatened Iraq to use military

---

321 TSAGOURIAS, N., "The prohibition of threats...", *op. cit.,* p. 80.

322 The UN Secretary-General's High-level Panel on Threats, Challenges and Change, UN, Doc. A/59/565, 2004, par. 188.

323 *Ibid*., par. 189-191; see also O'CONNELL, M. E.; EL MOLLA, R., "The prohibition on the use of force...", *op. cit.,* p. 318.

324 US, *Department of State Bulletin*, vol. XLVII, No. 1221, 12 November 1962, p. 717, available at https://archive.org/stream/departmentofstat471962unit/departmentofstat471962unit_djvu.txt, [visited on 5 June 2018].

325 See BRENNER, Ph.," Cuba and the Missile Crisis", *Journal of Latin American Studies.* 22(1), 1990, p. 115-142, at p. 117.

326 ROSCINI, M., "Threat of armed force...", *op. cit*., p. 237; and ICJ, *Legality of nuclear weapons, op. cit*., written statement of the Government of the French Republic, of 20 June 1995, declaration of lawful defensive military alliances even though they imply a deterrent threat, p. 25.

force if they did not withdraw. Only in the second case, the threats of force were lawful under the right of collective self-defence.

In this field, some scholars exaggerated the scope of the lawful threat of force. They claimed that there is no reason to assume that the threat will always be unlawful if under the same circumstances the resort to force would be illicit[327]. For instance they assert that even use of nuclear weapon in reality is not lawful (disproportionate in the right of self-defence), threat to use such weapons can be lawful if it is in the same line with the UN purpose attempt to maintain peace by discouraging an aggressor from probably aggression (nuclear deterrence). In other words, they expanded the definition of lawful threat of force, even over the scope of unilateral threats in the enforcement of collective security obligations and defensive threat. In fact, they claimed that the threat and use of force are uncoupled and threat is *sui generis* and for judge on their own merit does not need to refer to the use of force[328].

In this regard, Sadurska is pioneer in favour of broad definition of lawful threat of force. She asserts that a threat of sanctions to enforce another State to respect International Law or a threat to persuade to the resolution of a dispute, can be a lawful threat. Hence, certain threats for law enforcement purposes to maintain international peace and security are not necessarily unlawful. Then, according to Sadurska, the threat of force and the use of force are not treated equally, because the threat of force does not have the same destructive consequences as the use of force; as a result, from his standpoint, it is not rational to assume that the threat is always unlawful under the same circumstance in which the use of force is unlawful[329].

In fact, it is far of the mind that non-defensive threat that is not authorized by the UNSC can be an effective tool to maintain international peace and security. In reality, Sadurska's view

[327] SADURSKA, R., "Threats of Force…", *op. cit.*, p. 250.

[328] *Ibid*, p. 239-268.

[329] *Ibid,* p. 250.

on the threat of force was more political than legal and was finally disapproved by the ICJ in the *Legality of nuclear weapon*[330].

b) *Explicit and implicit unlawful threat of force*

The threat of force cannot be only explicit, it also can be implicit[331]. In this field, the ICJ in *Corfu Channel* case affirms that action by the British Navy had amounted to "a demonstration of force for the purpose of exercising political pressure" on Albania[332]. In this regard, several categories of threats are apparent in the State practice. Given the lack of a clear definition of threat of force in the international instruments and in the jurisprudence of the ICJ, scholars have attempted to clarify the concepts of unlawful threat of force by illustrating different types of threat of force. In this context, some authorities declared that the threat of force is "a message, explicit or implicit, formulated by a decision maker and directed to the target audience, indicating that force will be used if a rule or demand is not complied with"[333]. Also, Brownlie defined the threat of force as "an express or implied promise by a government of resort to force conditional on non-acceptance of certain demand of that government"[334]. Therefore, in accordance with the common point of definitions of threat, the threats of force can be explicit and implicit, and can include several types of threat, such as the *ultimatum* and other militarized acts that implicitly can constitute a threat of force.

The *ultimatum* is a clear communication (oral or *communiqué*) of explicit threat of force; that is along with demand, if threatened State refuses to the request, it ultimately gives rise

[330] ROSCINI, M., "Threats of armed force…", *op. cit.*, p. 255.

[331] EU, INDEPENDENT INTERNATIONAL FACT-FINDING MISSION ON THE CONFLICT IN GEORGIA (IIFFMCG), *Report*, vol. II, September 2009, p. 231, available at available at http://www.mpil.de/en/pub/publications/archive/independent_international_fact.cfm, [visited on 5 May 2018].

[332] See *Corfu Channel case* (United Kingdom *v.* Albania), judgment of 9 April 1949, *ICJ Reports 1949*, p. 35; see also, EU, INDEPENDENT INTERNATIONAL FACT-FINDING MISSION..., *op. cit.*, Vol. II, September 2009, p. 232.

[333] SADURSKA, R., "Threats of force...", *op. cit.*, p. 242.

[334] BROWNLIE, I., *International Law*…, *op. cit.*, p. 364.

to the use of force[335]. This kind of threat is simply recognized as a threat of force that most international academics refer to it. In this context, an ultimatum is "a communication issued by one State or group of States to another which threatens to employ coercive measures unless compliance with formulated demand is forthcoming within a certain time limit"[336]. Thus, ultimatum is more serious than a mere warning and has three component parts: i) specific demands, ii) a time limit for compliance, and iii) a threat of punishment or reprisal for failure to comply since disagreement with a demand will lead to a coercive measure[337].

In this type of threat, the demand has a fundamental role and a threat without a specific demand is a mere rhetorical dispute[338]. In this sense, a State insists on certain specific demands requiring unconditional acceptance. Hence, the demand is not only evidence to determine the threat of force and other criteria, such as sense of urgency, insistence and punishment by coercive measures are effectiveness to appear ultimatum threat of force[339].

In this regard, in the case of *Cyprus-Turkey* during 1963 to 1974, Turkey explicitly threatened to send its troops in December 1963 and this threat was backed up by Turkish navy and military plan in North of Cyprus. In this circumstance, Turkey threatened Cyprus to use of force unless Turkish Cypriot became under the protection of the president of Cyprus. Thus, if this threat was not justified in the right of self-defence, it seems that Turkey statements and actions were manifestations of threat of force that violated article 2(4). Nevertheless, the UNSC did not condemn Turkey's threat and asked to the parties to "exercise the utmost restraint in the present situation" and "to do everything in their power to reduce the present tensions"[340].

---

[335] GREEN, J. A.; GRIMAL, F., "The threat of force…", *op. cit*., p. 295; see also SEELOS, B., *The Anti-Secession Law…, op. cit.,* p. 36 where asserts that "the ultimatum is the strongest unlawful threat".

[336] LAUREN, P. G.,"Ultimata…", op. cit., p. 137.

[337] *Ibid*, p. 131-165.

[338] EU, INDEPENDENT INTERNATIONAL FACT-FINDING ..., *op. cit*., vol. II, September 2009, p. 232.WHITE, N; CRYER, R., "unilateral enforcement of Resolution 687: a threat too far", *Cal. W. Int'l LJ*, 29(2), 1999, p. 254.

[339] LAUREN, P. G., "Ultimata…", *op. cit*., p. 137.

[340] UNSC, Resolution 395 "Complaint by Greece against Turkey", of 25 August 1976, pars, 1 and 2.

The implicit threat of use of force has been prohibited in certain areas exclusively by treaties for peaceful purposes where they prohibited any measures of military nature, such as establishing military bases and fortifications, carrying out military manoeuvres as well as the testing of any type of weapons[341]. Hence, demonstrations of force by physical presence of military authority are a more considerable evidence to constitute a violation of article 2(4)[342]. The threat is mainly implied and created through fear that is not loud; then, is less transparent. However, it is assumed that militarized acts (such as military deployments, troop's build-up manoeuvres or tests) may provide signal readiness to use armed force against another State. Therefore, a threat is credible when it appears rational that it may be implemented, and not all militarized acts amount to an unlawful threat of force[343].

Naturally, demonstration of force depends on the circumstances of each case[344]. Militarized acts, when are conducted without hostile intention or in a routine mission, are lawful demonstrations of force. Out of these precedents, when they evidently are non-routine, scaled up, intensified and deducted potential military clash and geographically proximate, are unlawful demonstration of force[345]. For instance, the Turkish Strait Crisis in 1946 and Iraq troops deployment along with the Kuwait border on 6 October 1994 are examples of unlawful demonstration of force. In Iraq-Kuwait case, no State accepted that Iraq troops deployment and its exercises were in routine manner[346]. According to the threat's criteria, the majority of military exercises and the conduct of manoeuvres are under lawful demonstration of force, but States have the duty to announce their exercise in advance.

---

[341] For instance, article 1 of Antarctic Treaty, of 1 December 1959, and article 4 of the Outer Space Treaty, of 27 January 1967.

[342] EU, INDEPENDENT INTERNATIONAL FACT-FINDING ..., *op. cit*., vol. II, September 2009, p. 232.

[343] *Ibid;* STÜRCHLER, N., *The threat of force…, op. cit.,* p. 261.

[344] ILC, "Draft Code of crimes against the peace and security of mankind", *op. cit*., *Yearbook*, vol. I, 1989, p. 291; see also WALZER, M., *Just and unjust wars: A moral argument with historical illustrations*, 5th ed., Basic Books, 2015, p. 81.

[345] EU, INDEPENDENT INTERNATIONAL FACT-FINDING..., *op. cit*., vol. II, September 2009, p. 232; and STÜRCHLER, N., *The threat of force…, op. cit.,* p. 261.

[346] GREENHOUSE, S., "Threats in the Gulf: reaction; arab States withholding their support for baghdad", *New York Times*, 11 October 1994, *available at* https://www.nytimes.com/1994/10/11/world/threats-in-the-gulf-reaction-arab-states-withholding-their-support-for-baghdad.html, [visited on 1 July 2018].

3. *The restrictive approach to the threat of force under article 2(4) of the UN Charter*

In contrary to the prohibition of the use of force, there is a restrictive approach on the scope of the threat of force under article 2(4). In this sense, to breach the principle of the prohibition of the threat of force, the threat must have the characteristics to qualify as a threat of force under article 2(4).

a) *An identified threat*

The threat based on article 2(4) of the UN Charter is prohibited on the same basis and the same extent as the actual use of force. According to Corten, threat of force in article 2(4), on the one hand, can be constituted by a State against another State in specific situations (an identified threat, not a vague risk); it cannot be a general or fuzzy threat resulting from situation that might degenerate into a breach of peace. On the other hand, the threat has been clearly established, not being an uncertain threat, since this would not enter within the scope of the prohibition of article 2(4)[347]. In this direction, Schachter asserts that "a blatant and *direct threat* of force, used to compel another State to yield territory or to make substantial political concessions, would have to be seen as illegal under article 2(4)"[348]. Thus, according to threat of force in article 2(4), a restrictive conception prevails. It seems necessary to give a restrictive interpretation to what can be understood by "threat of the use of armed force"; otherwise, the possibility of the preventive self-defence would be opened[349]. If one of the preceding acts does not fall under the principle of the prohibition of the threat or the use of force, then it may constitute a violation of the principle of non-intervention in the internal affairs of other States.

In fact, threat in International Law has two separate meanings. Firstly, the threat under article 2(4) that prohibit the *threats of force* among States. Secondly, the *threat of peace* under article 39 of the UN Charter that authorizes the UNSC to take measure under Chapter

[347] CORTEN, O*., The law against war*…, *op. cit*., p. 94; see also RANDELZHOFER, A.; DÖRR, O., "Article 2(4)" , *op. cit*., p. 218; and GRIMAL, F., *Threats of force..., op. cit.,* p. 102 and 113.

[348] SCHACHTER, O., "The right of States to use armed force", *Michigan Law Review*, 82, 1984, p. 1625. (italic is ours)

[349] GONZALEZ, J. D., *et al*., *Curso de Derecho Internacional Público*, 4ª ed., Civitas, 2008, p. 1010.

VII. Threat under article 39 does not necessarily results from the threat of one State against another State, but also it derives from the breach of peace. Thus, there is a distinction between *threat of force* in article 2(4) and *threat of peace* under article 39. Contrary to the meaning of threat of peace under article 39 that has a broad meaning, such as humanitarian situations, floods of refugees or violation of peace agreements between States, the threat with meaning of article 2(4) contemplates one State against another with a hostile intention; only this kind of threat is covered by article 2(4)[350].

Also, the restrictive meaning of threat can be inferred from the declaration of the ILC envisaged in the definition of the crime "threat of aggression" on the grounds that threat was prohibited by article 2(4) [351]. In this context, the Commission stated:

> "As to meaning of the word 'threat' it must be pointed out that generally speaking the term may refer equally well to situations or disputes as to isolated acts. Thus it may be said of a situation that it constitutes a threat to international peace and security. That is so when situations or isolated acts in one region of the world contain germs of conflict liable to have repercussions on peace in that region and even in the rest of the world. It is not, however, in this sense that the word 'threat' is used in article 13 of the draft. Here, the world 'threat' denotes acts undertaken with the view to making a State believes that force will be used against it if certain demands are not met by that State"[352].

This distinction has also been revealed during debates around the 60th anniversary of the entry into force of the UN Charter. On one side, these debates indicated that threat is envisaged in an extremely broad sense as the path to action by both the UNSC and other UN organs[353], when threat derives from the outbreak of non-international armed conflict,

---

[350] See RUYS, T., "The meaning of 'force'...", *op. cit.*, p. 171-173.

[351] ILC, "Draft Code of Offences against the Peace and Security of Mankind", *op. cit.*, vol. II, part 2, 1989, p. 68.

[352] *Ibid*, par. 3.

[353] The UN High-level Panel on threat, challenges and changes, *op. cit.*, pars. 24-27, 44-58, 31-35, 74-88, 47-48, 145-46, 52-53, 165-170, 63-66, 44-58, and 31-35; UNGA, "In larger freedom: towards development,

deterioration of a humanitarian situation, cross-border movements of population or acute health problems. On the other side, threat has a narrow sense, in the context of rules related to the prohibition of the threat or use of force, when threat is confined to the outbreak of such prohibition by one State against another[354].

The mere supplying of arms might be threatening to international peace and security, but it does not constitute a threat of force against another State according to article 2(4)[355]. This allegation is revealed in the precedent of the missile crisis between the US and Cuba in 1962, where the US accused Cuba's activity to threat the peace of hemisphere, and of the world[356]. The US for convincing and obtaining a resolution from the Organization of American States (OAS) to take the necessary measures, asserted that Cuba's offensive arms were an "active threat to the peace and security of the continent"[357]. In this circumstance, the US did not refer to the prohibition of the threat of force set out in article 2(4) and any State claimed that accepting weapons and its installation in territory of Cuba had violated the rule[358]. Likewise, several States asserted that quarantine measure by the US against any vessel which was threatened by coercive action was the violation of the prohibition of threat of force enshrined in article 2(4)[359]. Other States considered those measures consistent with the Chapter VII without denying that there was a threat of force[360].

---

security and human rights for all", Report of the Secretary -General, U.N., Doc. A/59/2005, of 21 March 2005, pars. 77-81; and World Summit Outcome, UNGA Resolution 60/1, of 16 September 2005, pars. 69-72 and 79.

354 UN Security General High level-Panel, *op. cit.*, 2004, par. 188; *In larger freedom: op. cit.*, par. 124; and World Summit Outcome, UNGA Resolution 60/1, *op. cit.*, par. 77.

355 CORTEN, O., *The law against war…, op. cit.,* p. 96; see also SEELOS, B., *The anti-secession law…, op. cit.,* p. 36.

356 US, UN, Doc. S/PV.1022 on Cuba, of 23 October 1962, par. 14; see also pars. 74, 79 and 82.

357 OAS, Resolution of 23 October 1962, UN, Doc. S/5193, 3, par. 2; see also UN, Doc S/5182, of 23 October 1962.

358 Venezuela, UN, Doc. S/PV.1023, 24 October 1962, par. 7; and France, UN, Doc. S/PV. 1024, 24 October 1962, par. 10.

359 Cuba, UN, Doc. S/PV.1022, of 23 October 1962, pars. 88, 110, and 122-23; USSR, UN, Doc. S/PV.1023, pars. 157-58, 173; and S/5187; Romania, UN, Doc. S/PV.1023, of 24 October 1962, par. 58; and UAR (United Arab Republic), UN, Doc. S/PV.1024, of 24 October 1962, par. 67.

360 France, UN, Doc. S/PV.1024, 24 October 1962, para10; China, UN, Doc. S/PV.1024, 24 October 1962, par. 18); and USA, UN, Doc. S/PV.1025, of 25 October 1962, pars. 15,16.

Another precedent to distinguish between the restrictive sense of the threat of force in article 2(4) and the broad sense of the threat to peace under article 39 of UN Charter is related to Israel-Iraq event in 1981. Israel's attack to Iraq nuclear installations in 7 June 1981, along with multiple threats to destroy other installations of Iraq and of its neighbouring States, was condemned in several UNGA resolutions by large majorities[361].

Moreover, in relation to the alliance treaties, a State may asserts that it implicitly be threatened by entering rival State into a defensive alliance treaty such as the case of Russia with the Georgia and Ukraine's accession to NATO[362]. In this regard, distinguish between defensive and offensive purpose of treaties is not easy, since it is difficult to accept that an alliance treaty can threaten a State, without directly targeting such State[363].

Thus, threat under article 2(4) has a restrictive meaning and must be directed against another State in an unlawful situation[364]. In this sense, threat must be conducted against specific States to qualify threat under article 2(4)[365]. In the situation where the threat is simply dangerous for international peace and security, the threat does not necessary violate article 2(4). However, it does not mean that the UNSC does not have competence to manage any situation that may threats the international peace and security.

---

[361] UNGA, Res. 36/27, of 13 November 1981, preamble and par. 2; UNGA, Res. 37/18 of 16 November 1982 preamble and pars. 3-4; UNGA, Res. 38/9, of the 10 November 1983, pars. 2-4 and 6; UNGA, Res. 39/14, of 8 November 1984, pars. 2-4; UNGA, Res. 40/6, of 1 November 1985, pars 2 and 4, UNGA, Res. 41/12 of 29 October 1986, par. 2; see also UNSC Res. 487, of 19 June 1981, par. 2.

[362] OSBORN, A., "Putin warns NATO against closer ties with Ukraine and Georgia", *Reuters*, 19 July 2018, available at https://www.reuters.com/article/us-russia-nato-putin/putin-warns-nato-against-closer-ties-with-ukraine-and-georgia-idUSKBN1K92KA,]visited on 8 August 2018[.

[363] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit.*, p. 218; see also GRIMAL, F., *Threats of force: International Law and strategy*, Routledge, 2013, p. 43.

[364] RANDELZOLFER, A.; DÖRR, O., "Article 2(4)" , *op. cit.*, p. 218.

[365] INDEPENDENT INTERNATIONAL FACT-FINDING MISSION..., *op. cit.*, vol. II, September 2009, p. 232-233.

b) *The hostile intention*

As it was previously mentioned, the threat of force can result explicitly and implicitly from militarized acts as a demonstration of force by military deployments, troop build-up and manoeuvres or tests that signalled readiness to recourse to use of armed force against another State. Then, military manoeuvres and other military activities *per se* can not violate the threat of force without hostile intention[366]. In fact, intention infers from article 2(4) of the prohibition of force from one State against another State. Thus, criteria of intention must exist in the threat to violate the principle of the prohibition of the threat of use of force[367]. In this sense, the threat of force does not include any behaviour; threat must be determined on a case by case basis clearly attending their particular circumstances.

At this point, we have to ask ourselves whether the acquisition of weapons by one State is a threat of force under article 2(4) against another State or not. In fact, regarding the ICJ advisory opinion on the *Legality of Nuclear Weapons*, Stürchler asserts that the acquisition of nuclear weapons may constitute a threat of force if other criteria are met. In addition to that, from the endeavour of States to gain control of arms from partial weapon ban regime, it is deduced that States have the right to acquire weapons as long as it is not against the non-proliferation treaty (NPT)[368]. Therefore, the mere acquisition of specific weapons can neither be seen as a threat of force nor as a breach of article 2(4), since it requires more than the ownership of arms[369].

Likewise, the relevance of the intention to threat is confirmed by some members of the ILC whom deduce that intention is different from motivation[370]. Whereas motivation is the

---

366 R0SCINI, M., *Threats…*, *op. cit*., p. 240; see also ICJ, *Legality of nuclear weapons, op. cit.,* Memorial of Government of Nauru on Nuclear Weapon, of 15 June 1995, p. 26.

367 CORTEN, O. *The law against war…, op. cit.,* p. 100; and RANDELZHOFER, A.; DÖRR, O., "Article 2(4)" , *op. cit*., p. 218, in this sense, Randelzhofer and Dörr asserts that threat need to "a coercive *intent* directed towards specific behavious on the part of another State"(italic is ours).

368 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), of 1 July 1968.

369 STÜRCHLER, N., *The threat of force…, op. cit.,* p. 263; see also dissenting opinion of judge Weeramantry in ICJ, *Legality of nuclear weapons, op. cit*., p. 540.

370 ILC, "Draft Code of crimes against peace and security of mankind", Summary records of the meetings of the forty-first session, *Yearbook of ILC,* vol. 1, 1989, article 13, p. 19.

reason for an act of aggression to destruction, annexation and other hostile acts against a State, intention exists when a State is committing the act deliberately[371].

In addition to that, the importance of intention has been confirmed in the *Nuremberg Judgments* and the subsequent proceedings for determining whether a specific conduct is a threat of force under article 2(4) or not. In *German High Command Trial,* the US Military Tribunal mentioned that "[…] as long as there is no aggressive intent, there is no evil inherent in a nation making itself military strong"[372]. As a result, hostile intentions between concerned States have the fundamental role to ascertain whether explicit or implicit conduct can be qualified as a threat of force according to article 2(4)[373].

Regarding the judicial precedents, militarized acts without hostile intention are not threat of force by article 2(4), especially when these threats are non-routine, scaled up, and geographically proximate[374]. This approach has been revealed by the ICJ in the *Corfu Channel* and *Nicaragua* cases.

In the *Corfu Channel* case, regarding the passage of four British warships through the Channel in 22 October 1946 that resulted in a mine accident, the Court denied Albania's assertion that the passage of warships showed an intention to intimidate and not merely to pass, mentioning that

> "The intention must have been, not only to test Albania's attitude, but at the same time to demonstrate such force that she would abstain from firing again on passing ships. Having regard, however, to all the circumstances of the case, as described above, the Court is unable to characterize these

371 *Official Records of the UN General Assembly, Seventh Session, Annexes*, agenda item 54, U.N. Doc. A/2211, of 3 October 1952, p. 68.

372 US MILITARY TRIBUNAL V, *High command trial,* United States of America *vs*. Wilhelm von Leeb *et al*., judgment of 27 October 1948, *Trials of War Criminals Before the Nuremberg Military Tribunals*, vol. IX, p. 487.

373 ROSCINI, M., "Threats of armed force…", *op. cit*., p. 242.

374 STÜRCHLER, N., *The threat of force…, op. cit.,* p. 261.

measures taken by the United Kingdom authorities as a violation of Albania's sovereignty"[375].

In the *Nicaragua case*, Nicaragua claimed that the continuous US military and naval maneuvers near Nicaragua's frontier amounted to the threat of force under article 2(4), which constitutes a policy of force to intimidate the Nicaragua government in order to accept the US political demands which violate Nicaragua's political independence[376]. However, the ICJ denied Nicaragua's claims and held that US military maneuvers did not amount to violate article 2(4)[377]. At this point, although Nicaragua submitted sufficient evidence (such as the US financial proposal) to the US's contribution to the *Contra,* it had to accept certain demands from the US. The ICJ rejected Nicaragua's claim and characterized the sending of funds only as a violation of principle of non-intervention, discarding the violation of the prohibition of the threat of force[378].

The US President Speech on 4 April 1985, by declaring "the non-threat of manoeuvre against anyone" attempted to emphasize on any hostile intention in its maneuver. Then, military maneuver should be accompanied by a declaration of non-threat, and it cannot be a threat even in situations where there is an extreme tension between the concerned States[379]. This approach also has been affirmed by the *Independent International Fact-Finding Mission on the Conflict in Georgia* (IIFFMCG) which was established to investigate the Russia-Georgia conflict in 2008[380]. This institute mentioned that "[…] according to State practice […] not all militarized acts amount to a demonstration of force and thus to a violation of article 2(4) of the UN Charter. Many are routine missions devoid of any hostile intent and are meaningless in the absence of a sizable dispute" [381]. Similarly, it referred that "[…] secret military exercises or manoeuvres might amount to the preparation of

[375] ICJ, *Corfu Channel case, op. cit.*, p. 31.

[376] ICJ, *Nicaragua case, op. cit.*, par. 92.

[377] *Ibid*., par. 227

[378] *Ibid*, pars. 118 and 292.

[379] CORTEN, O., *The law against war…, op. cit.,* p. 103.

[380] EU, INDEPENDENT INTERNATIONAL FACT-FINDING..., *op. cit.,* Vol. II, September 2009, p. 232.

[381] *Ibid*, p. 232.

aggression but are not threats under the terms of article 2(4) if they are unknown to the victim"[382]. It declared as soon as militarized acts "are non-routine, suspiciously timed, scaled up, intensified, geographically proximate, staged in the exact mode of a potential military clash, and easily attributable to a foreign policy message, the hostile intent is considered present and the demonstration of force manifest"[383]. Then, it is comprehendible that all demonstration of force does not amount to a threat of force of article 2(4), if it holds in routine mission and there is not a hostile intention of the threatening State.

In this context, a clear example to exist a hostile intention of the threat of force is the deployment of Iraqi artillery and tanks in the border of Kuwait in 1990. In this regard, the UK and New Zealand representative in the UNSC cited that deployment of Iraq artillery with sophisticate weaponry in the border of Kuwait amounts to an aggressive threat to Kuwait and to a violation of article 2(4) by invoking that Iraq had a stubborn behaviour to recognize Kuwait sovereignty[384].

Moreover, the recourse to hostile intention criteria has frequently been used by plaintiff States to convince that another States violated the prohibition of the threat of use of force. For instance, Libya argued that the US and the UK Declaration of 1991-1992 is *pattern of threat* by consideration to a background and bombing Libyan cities in 1986[385]. Also, recently, Iran qualified the US statements as a threat of force and probability of use of force in regard to past illegal behaviours against this State[386].

Thus, in order to the violation of the article 2(4), there is a restrictive approach on the threat of the use of force. As a result, a State must go further than the simple threat expression or military activities to violate the prohibition of the threat of force under

[382] ROSCINI, M., "Threat of armed force...", *op. cit*., p. 237-238.

[383] THE COUNCIL OF THE EUROPEAN UNION*,* Concerning an Independent*..., op. cit*., vol. II, p. 232.

[384] UNSC, Doc. S/PV.3438, of 15 October 1994, p. 9 and 11.

[385] ICJ, Declaration by I. Brownlie, Counsel for Libya, Lockerbie, Preliminary Objections, Verbatim Record, CR 97/21, 17 October 1997, p. 51, available at http://www.ruhr-uni-bochum.de/www-public/fischhcy/ICJ/E309.htm, [visited on 2 June 2018].

[386] Latter dated in 17 March 2006 by permanent representative of Iran to the UN Secretary–General.

article 2(4). A mere, military alliance or maneuver cannot breach article 2(4)[387]. In other words, the threat must be actively attempting to intimidate other States by specific threats, such as concentration of troops and the removing or the displaying of forces along with the precedent hostile intention between concerned States. Therefore, the hostile intention is a significant criteria or requirement to determine the existence of the threat of use of force under article 2(4).

Also, in this field, there exists other requirements relevant to the threat to give credibility to such threat of force as specific demands, deadline for a reply, imminent danger and fear, but identified threat and a hostile intention are significant requirements that are necessary to give credit a threat under article 2(4).

D. **Exceptions to the principle of the prohibition of the threat or use of force**

As we have seen, article 2(4) of the UN Charter forbids the use of force. This means that the Charter had to establish alternative mechanisms to allow States to react against possible violations of the prohibition of the threat or use of force. In this sense, the Charter prescribes two exceptions to such prohibition. The first one works in the framework of the *collective security system* which includes the actions adopted by the UNSC pursuant to Chapter VII of the UN Charter; the second one is related to the *right of individual or collective self-defence* against an armed attack enshrined in article 51 of the UN Charter as a subsidiary proceeding of such collective security system. A third exception to the prohibition of the use of force not predicted in the UN Charter is the use of force by NLM justified in the context of the right of peoples to self-determination.

In continue, we are going to make a brief reference to the UN enforcement actions under Chapter VII of the UN Charter, and to the use of force by the NLM. In Chapter II we will analyze the individual or collective right of self-defence against an armed attack recognized in article 51 of the UN Charter.

[387] STÜRCHLER, N., *The threat of force…, op. cit.,* p. 264.

1. *UN enforcement actions pursuant to the Chapter VII of the UN Charter*

The first exception is posed in Chapter VII of the Charter (articles 39-50) where lawful use of force is provided by article 42, whereby the UNSC may authorize the use of force, for instance taking military enforcement measures. This force can be implemented in three different ways: i) in accordance with article 43 of the UN Charter, where UN members are undertaken to provide available force and assistance for the UNSC with agreement in purpose of maintaining peace and security. Until now, States have not had any agreement[388]; ii) according to article 48(2) of the UN Charter, the decisions of the UNSC authorizing the use of force can be "carried out by the members of the United Nations directly and through their action in the appropriate international agencies of which they are members"; and iii) the UNSC for enforcement actions under its authority can also utilize regional arrangements or agencies as it is predicted under article 53 of the UN Charter, where there are two types of situation; in the first one, the UNSC assumes the initiative of utilizing these regional arrangements or agencies and, in the second one, the initiative to take an enforcement action derives from the regional agency, but such action is only allowed on the basis of the UNSC authorization[389].

2. *The use of force by National Liberation Movements* (NLM)

As it has seen *supra*, the UNGA Resolution 1514 (XV) proclaimed the right to self-determination of all colonial peoples. Therefore, according to paragraph 4 "all armed action or repressive measures of all kinds directed against dependent people shall cease in order to enable them to exercise peacefully and freely their right to complete independence"[390].

---

[388] SUTTERLIN, J. S., *The United Nations and the maintenance of international security: a challenge to be met*, Greenwood Publishing Group, 2003, p. 54.

[389] See VILLANI, U., "The Security Council's authorization of enforcement action by regional organizations", *Max Planck Yearbook of United Nations Law online,* 6(1), 2002, p. 535-555, available at http://booksandjournals.brillonline.com/content/journals/10.1163/138946302775159352, [visited on 25 June 2018].

[390] UNGA, Resolution 1514 (XV), *op. cit*., par. 4.

The use of force by people in favour of right of self-determination cannot be considered contrary to the general prohibition of use of force because it is legitimized to be at the service of a general right, inalienable, fundamental, recognized and confirmed by the international community, for instance, in UNGA Resolutions 1514 (XV), 1541 (XV) or 2625 (XXV).

Some authorities affirm that the use of force by the NLM is a particular case of right of self-defence related to the use of force by colonial peoples (or NLM) to exercise its right of self-determination[391]. In this sense, they allege that people deprived of their right of self-determination by force, are entitled to use force as an exception to the prohibition of the use of force by resorting to the right of self-defence[392].

However, according to UNGA Resolutions 2625 (XXV), 3314 (XXIX) and 42/22,

> "the positions of the States expressed in the negotiations prior to them demonstrate the existing reluctance to include more explicit references to the nature of the right of colonial peoples to take up arms against their oppressor, which supports the idea that, in effect, that fight should not be framed in article 51 of the Charter"[393];

In other words, the right of colonial peoples to use force is not included in the right of self-defence. Thus, such right is an exception *sui generis,* categorized as *ius cogens* norm, to the prohibition of the use of force, not explicitly incorporated in the UN Charter[394].

---

[391] ICJ, *Legal consequences for States of the continued presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (197*0), advisory opinion of 21 June 1971, *ICJ Reports* 1971, separate opinion of judge Ammoun, that affirmed that the legitimacy of one people to fight to exercise its independence "follows from the right of self-defence, inherent in human nature, which is confirmed by article 51 of the United Nations Charter", p. 70.

[392] IGLESIAS, J. L., "La prohibición general del recurso a la fuerza i las resoluciones descolonizadoras de la Asamblea General de las Naciones Unidas", *REDI*, 24, 1971, p. 173-201, at p. 200; RÖLING, B. V. A., "Aspects of the ban on force", *NILR,* 24, 1977, p. 242-259 at p. 243-244; GRAHL-MADSEM, A., "Decolonization: the modern version of a 'just war'", *BYIL,* 22, 1979, p. 255-273, at p. 255-269; and CASSESE, A., *International Law,* OUP, 2005, p. 347.

[393] CERVELL, M. J., *La legítima defensa..., op. cit*., p. 39; see also p. 37-40.

[394] *Ibid,* p. 40.

While the use of force by colonial peoples in favour of self-determination is clearly according to International Law, now the question is whether it is lawful or not to give support to colonial peoples or NLM by other States. Resolution 2160 (XXI), in its Preamble, mentioned that "Recognizing that peoples subjected to colonial oppression are entitled to seek and receive all support in their struggle which is in accordance with the purposes and principle of the Charter", and in article 2(b) "Urgently appeals to States, to exert every effort and to undertake all necessary measures with a view to facilitating the exercise of the right of self-determination of peoples under colonial rule, lessening international tension, strengthening peace and promoting friendly relations and co-operation among States"[395].

Moreover, in the Drafting Committee of the UNGA Resolution 2625 (XXV), two alternatives were discussed: i) on the one hand, the majority of States supported that any government of any State may use any means (weapons, financial resources or direct aid such as sending troops) to help NLM which are fighting in order to achieve self-determination; for instance, the most Non-Aligned States and the Socialist States; ii) on the other hand, the US and other Western States disagreed on any outside military intervention in an armed conflict in support of NLM[396]. At the end, the Resolution 2625 (XXV) declared that every State has the duty to refrain from any forcible action which deprives people of their right to self-determination "in their action against, and resistance to, such forcible action in pursuit of the exercise of their right to self-determination, such peoples are entitled to seek an to receive support in accordance with the purposes and principles of the Charter"[397].

[395] UNGA Resolution 2160 (XXI) "Strict observance of the prohibition of the threat or use of force in international relations, and of the right of peoples to self-determination", 30 November 1966.

[396] US, UN, Doc. A/AC.119/SR.15, 8 September 1964, p. 19; UN, Doc. A/AC.119/SR.17, 9 September 1964, p. 17; Venezuela, UN, Doc. A/AC.119/SR.16, 9 September 1964; Canada, UN, Doc. A/AC.125/SR.23, 24 March 1966, par. 36; UN, Doc. A/AC.125/SR.66, 1 August 1967; Mexico, UN, Doc. A/AC.125/SR.66, 1 August 1967, France, *Report of the special Committee on Principles of international law concerning Friendly relations and co-operation among States,* supp. no 18, A/8018, 1970, par. 149, UK, UN, Doc. A/AC.134/SR. 11, 18 June 1968 in A/AC.134/SR.1-24; A/AC.134/SR.55, of 16 July 1970 in A/AC.134/SR., p. 52-66; and A/AC.134/SR.85, of 9 February 1971 in A/AC.134/SR., p. 79-91.

[397] UNGA, Resolution 2625 (XXV), *op. cit.*, par. 5 of the principle of equal rights and self-determination of peoples.

Similar statements have been reaffirmed by other resolutions, such as article 7 of the Resolution 3314 (XXIX) and the Resolution 36/103[398] which emphasize that nothing can deprive peoples from the right of self-determination, freedom and independence. Thus, the right of self-determination includes a set of faculties in favour of colonial peoples and among them, the right to fight against the State which denies their right to self-determination.

Although part of the doctrine affirms that the support provided by third States to NLM is limited to political, humanitarian or economic assistance to achieve their right of self-determination[399], other authors understand that such assistance can also include the supply of arms, military material or even logistical support during the conflict[400]. Also, the last approach seems to be implicit in the *Nicaragua case* where the Court refused the legality of the intervention of the States in support of the parts in a domestic conflict but explicitly excluded those who refused the process of decolonization "The Court is not here concerned with the process of decolonization; this question is not in issue in the present case"[401]. Thus, "excepting a concrete assumption, in a context of rejection of similar situations can be interpreted clearly as an indirect affirmations of the legality of interventions in support of decolonization processes"[402]. Moreover, the UNGA Resolution 35/227 A, relating the illegal occupation of Namibia by South Africa, legitimizes the struggle of the Namibian people with "all means at their disposal, including the armed struggle", and not only urging the States to provide material and financial assistance, but also "military" aid[403].

---

[398] UNGA Resolution 36/103 "Declaration on the Inadmissibility of and Interference in the Internal Affairs of States", 9 December 1981.

[399] ICJ, *Nicaragua case, op. cit.,* dissenting opinion of judge Schwebel, p. 350-351; DINSTEIN, Y., *War, aggression..., op. cit.*, p. 73-75; and CORTEN, O., *The law against war..., op. cit*., p. 143-145.

[400] GUTIÉRREZ, C., *El uso de la fuerza y el Derecho Internacional después de la descolonización,* Universidad de Valladolid, 1988, p. 42-43; CASSESE, A., *Self-determination of people: legal reappraisal,* CUP, 1999, p. 199; and RODRIGUEZ, A. J., *Lecciones de Derecho Internacional Público*, 5th ed., Tecnos, 2002, p. 608-609.

[401] ICJ, *Nicaragua case, op. cit*., par. 206.

[402] RODRIGUEZ, A. J., *Lecciones de Derecho…, op. cit.,* p. 609.

[403] UNGA, Resolution 35/227 A on "question of Namibia", 6 March 1981, par. 3 and 6.

The practice has been that States can help with financial resources or supply of weapons to NLM, but cannot send troops directly; in fact, there has never been a military intervention of a third State in cases of struggle for the self-determination of colonial peoples. Normally, what third States did, was sending official military instructors or military techniques or mercenaries.

Therefore, it is necessary to point out that it is very doubtful that third States may use the force by intervening in these conflicts in favour of the NLM[404]. However, they can give support to these movements with political, economic or technical assistance, supplying military material or sending mercenaries, "in accordance with the purposes and principles of the Charter", as indicated in the UNGA Resolution 2625 (XXV).

[404] CASANOVAS, O., "El principio...", *op. cit,* p. 1085.

CHAPTER II

THE RIGHT OF SELF-DEFENSE IN INTERNATIONAL LAW

A. General considerations and characteristics of the right of self-defence

1. *Individual and collective right of self defence*

According to article 51 of the UN Charter

> "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".

The right of self-defence, which was already explicitly or implicitly legitimated as an exception in earlier legal instruments such as Kellogg-Briand Pact[405], recognizes the inherent right of individual or collective self-defence against an armed attack. In accordance with article 51 of the UN Charter, the right of self-defence may be individual or collective. In fact, article 51 of the UN Charter reassures the UN member States, provided that if the enforcement machinery of the UN were to fail, they would legally be authorised to use force under the right of self-defence[406]. This individual or collective right of self-defence is also part of general International Law as declared by the ICJ[407]. As seen *infra,* the

[405] HIGGINS, N., *Regulating the use of force…, op. cit.,* p. 42; and KU, Ch.; JACOBSON, H. K. (eds.), *Democratic accountability and the use of force in International Law*, CUP, 2002, p. 13.

[406] HIGGINS, *ibid.*

[407] ICJ, *Nicaragua case, op. cit*., pars. 176 and 193; and *Oil Platform* case, *op. cit*., pars. 39 and 51.

individual self-defence authorizes any State[408] (member or non-member of the UN) to resort to the use of armed force by the essential right of defence against aggressor States.

The collective self-defence has two modalities: first, in the framework of a previous compromise in a bilateral or multilateral treaty of mutual self-defence or military alliance, and second, through a prior and urgent request by a State which has been victim of an armed attack from other States. In relation to the first modality, there are various treaties that expressly establish collective reactions in the event that one of the State parties is the target of an armed attack and regulate the conditions in which such States agree to provide assistance. For instance, article 5 of the *NATO* of 4 April 1949, article 42(7) of the *European Union Treaty* of 7 February 1992 or article 2 of the *Treaty of Joint Defence and Economic Cooperation between the States of the Arab League* of 17 June 1950[409].

According to the second modality, the exercise of the collective right of self-defence needs two requirements established by the ICJ in the *Nicaragua case*: firstly, the State that suffers the armed attack *must declare* itself a victim and it only corresponds to him to assess whether or not there has been an armed attack and go to another State or States in search of help[410]; and secondly, the victim State of an armed attack has to *request help* based on the right of self-defence[411]. Of course, the other requirements, such as necessity, proportionality[412], immediacy or the notification to the UNSC of the action adopted, must be all met.

---

[408] ICJ, *Nicaragua case, op. cit*., pars. 50-52 and 224; and *Oil Platform case*, *op. cit*., pars. 62 and 37-40.

[409] See DINSTEIN, Y., *War, aggression…, op. cit*., p. 306-312; and CERVELL, M. J.*, La legítima defensa*…, *op. cit*., p. 150-160.

[410] ICJ, *Nicaragua case, op. cit*., par. 195.

[411] *Ibid*, par. 199; and *Oil Platform case, op. cit.,* par. 51. Also the requirement of the request is clearly reaffirmed by IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", Tenth Commission, 27 October 2007, *Annuaire de l'Institut de Droit International,* vol. 72, article 8; and by *Tallinn Manual 2.0*, *op. cit.,* rule 74, pars. 2 and 3. Moreover, State practice has confirmed this condition, for instance Vietnam with US in front the aggression suffered in 1965 by the North, UN, Doc. S/6174, 7 February 1965; and Kuwait in 1990 against Iraq aggression, see DINSTEIN, Y., *War, aggression…, op. cit*., p. 345-346.

[412] ICJ, *Nicaragua case, op. cit*., par. 237 and *Oil Platform case, op. cit.,* par. 51.

In practice, the collective security system envisaged in the San Francisco Conference, which has not worked during the cold war due to the right of veto from UNSC permanent members, has been replaced by a system of collective self-defence. This is one of the major changes in the forecasts of the UN Charter[413]

2. *Nature and foundation of the right of self-defence*

The essence of self-defence is self-help, where self-help has been a feature of all primitive legal systems[414]. In ILC wording, "Self-defence' may therefore be regarded as a form of 'armed self-help or self-protection' that, under modern International Law, States are permitted to exercise directly"[415]. The right of self-defence is a fundamental right that is recognized in customary and practice of nations, also called *law of nations* or *customary international law*. "The UN Charter, the most important codification of those customs and practices, did not create the right, nor does it limit it"[416].

In accordance with the French version of the UN Charter and the ICJ, the right of self-defence is an inherent right (*droit natural*) [417]. In fact, the practice and *opinio iuris* of States which mainly manifest in the UNSC, have given rise to a customary law on how to carry out a self-defensive action. According to some authors, article 51 crystallized the customary norm[418]. In fact, the customary self-defence coexists with the conventional self-defence in article 51 of the UN Charter. As the ICJ stated "article 51 of the Charter is only meaningful on the basis that there is a 'natural' or 'inherent' right of self-defence, and it is hard to see

[413] PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 667.

[414] DINSTEIN, *War, aggression*…, *op. cit.,* p. 202.

[415] ILC, "State responsibility", *op. cit.,* vol. ll, part 2, 1980, p. 54.

[416] US, DoD, OFFICE OF GENERAL COUNSEL, *Legal Distinction between preemption, preventive self-defense and anticipatory self-defense*, report from HAYNES, W. J., 16 October 2002, p. 1, available at http://library.rumsfeld.com/doclib/sp/2564/2002-10-16%20from%20William%20Haynes%20re%20Legal%20Distinction%20Between%20Preemption,%20Preventive%20and%20Anticipatory%20Self-Defense.pdf, [visited on 1 March 2018].

[417] ICJ, *Nicaragua case*, *op. cit*., par. 176.

[418] BROWNLIE, I., *International Law*…, *op. cit.,* p. 19, 40, 84 and 231; CASSESE, A., "Article 51", in COT, J. P., *et al*. (eds.), *La Charte des Nations Unies. Commentaire article par article*, 3rd ed., Economica, 2005, p. 1329-1360, at p. 1331; and REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 672.

how this can be other than of a customary nature, even if its present content has been confirmed and influenced by the Charter"[419]. However,

> "it cannot therefore be held that article 51 is a provision which 'subsumes and supervenes' customary International Law. It rather demonstrates that in the field in question, the importance of which for the present dispute need hardly be stressed, customary International Law continues to exist alongside treaty law. The areas governed by the two sources of law thus do not overlap exactly, and the rules do not have the same content"[420].

In this context, some States and authors support to expand the scope of application of this right, maintaining that customary self-defence coexists, and it is wider than the self-defence of the UN Charter[421].

The right of self-defence is also implicitly recognized in UNGA Resolutions 2625 (XXV) and 3314 (XXIX), and explicitly reaffirmed in UNGA Resolution 42/22 which declared that "States have the inherent right of individual or collective self-defence if an armed attack occurs, as set forth in the Charter"[422].

Which is the foundation of the right of self-defence? To maintain the existence of the State is the main purpose as expressed in article 51 of the UN Charter. Self-defence is a consubstantial right to the sovereignty of the State which implies the first rule of State to ensure its survival as such. In this sense, the ICJ declared that "the Court cannot lose sight of the fundamental right of every State to survival, and thus its right to resort to self-defence, in accordance with article 51 of the Charter, when its survival is at stake" [423].

---

[419] ICJ, *Nicaragua case*, *op. cit.*, par. 176.

[420] *Ibid.*

[421] For instance see, WALDOCK, C. H. M., "The regulation of the use of force by individual States in International Law", *RCADI*, 2, 1952, p. 451-517, at p. 495-515; BOWETT, D. W., *Self-defence..., op. cit.,* p. 185-186 and SCHWEBEL, S. M., "Aggression, intervention and self-defence in modern International Law", *RCADI*, 2, 1972, p. 411-497, at p. 479-497.

[422] UNGA, Resolution 42/22, *op. cit.*, par. 13.

[423] ICJ, *Legality of nuclear weapons, op. cit.*, par. 96.

Moreover, the right of self-defence is integrated into the collective security system. Article 51 does not create a right of self-defence, but expressly recognizes its existence and its compatibility with the collective action mechanism which is established in the UN Charter against offenders. In fact, the collective security system combines a global peacekeeping mechanism, which "confer on the Security Council primary responsibility for the maintenance of international peace and security"(article 24), with an alternative self-defensive mechanism based on the States considered individually or collectively (article 51). In other words, self-defence "reflects the lack of absolute ability of the UN to maintain international peace and security"[424] in the cases that the function of the collective security system is blocked.

In this context, article 34 of ILC *Draft articles* in its first reading in 1996 approved self-defence as circumstance excluding a wrongful act[425]. In the comment of the *Draft articles*, ILC emphasized that self-defence implied *per se* the use of armed force, but it differentiated it from other excluded circumstances set out in the *Draft*[426]. The main difference between the right of self-defence and others causes admitted in International Law to exclude an illicit one, putting aside the different requirements of each of these figures, is that the self-defence expressed under article 51 of the UN Charter is part of a primary norm. In this regard, Thouvenin claims that the objective of the ILC is not to codify self-defence as primary International Law which is placed in the UN Charter, but as a special circumstance that excludes it from an illegal act[427]. Therefore, the State that acts in self-defence does not act contrary to the Charter; as a result, an illegal international act has not been committed. Consequently, self-defence is a circumstance of exclusion of the illicit.

---

[424] KUNZ, J. L., "Individual and collective self-defence in article 51 of the Charter of the United Nations", *AJIL*, 41(4), 1947, p. 872-879, at p. 874.

[425] According to ILC "the wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the at constitutes a wrongful measure of self-defence taken in conformity with the charter of the UN Nations", see ILC, "Draft articles on State responsibility", *Yearbook of ILC*, vol. II, part 2, 1996, p. 62.

[426] ILC, *Draft articles on State Responsibility with commentaries thereto adopted by the International Law Commission on First Reading*, January 1997, p. 260.

[427] THOUVENIN, J. M., "Circumstances precluding wrongfulness in the ILC article on state responsibility: self-defence", in CRAWFORD, J., *et. al*. (eds.), *The law of international responsibility*, OUP, 2010, p. 455-468, at p. 460-461.

In fact, "self-defence is a concept clearly shaped by the general theory of law to indicate the situation of a subject of law driven by necessity to defend himself by the use of force against the attack by another"[428]. It also indicates that the intention of the *Draft articles* was neither to define nor to codify the right of self-defence since "the right of self-defence is a principle recognized both in the Charter of the United Nations and in contemporary International Law […]"[429].

Moreover, in 2001 ILC a new change was made in article 21 of the *Draft articles*, regarding the right of self-defence, asserting that "the wrongfulness of an act of a State is precluded if the act constitutes lawful measure of self-defence taken in conformity with the Charter of the United Nations". In its commentary, the ILC emphasized that no one discuses that the self-defence is an exception to the prohibition of the use of force in international relations, but pointed out that this does not imply that self-defence excludes the unlawful of a behaviour in any circumstance or in front of any obligation, mentioning as examples the obligations of due compliance with the rules of IHL and human rights that do not allow derogation[430].

In this regard, Gutiérrez emphasized that the self-defence was included in article 21 of the ILC *Draft*, so that the victim State would not have to comply with the international treaties that commit to it with the aggressor State or with third parties, except for the international treaties of IHL, those who consecrate to the hard core of human rights (life, prohibition of torture, racial discrimination, etc.) and treaties on the environment that have been adopted to be fulfilled in any circumstance[431].

Pellet, in relation to article 26 of the *Draft articles* regarding compliance with imperative rules, adds that this article imposes in any case respect for the rules of *ius cogens*. This means that a State cannot respond to serious violations of imperative rules committing a

---

[428] ILC, *Draft articles on State responsibility with..., op. cit.,* January 1997, p. 260.

[429] *Ibid*, p. 266.

[430] ILC, "Draft articles on responsibility of states for internationally wrongful acts, with commentaries", *Yearbook of ILC,* vol. II, part 2, 2001, p. 74.

[431] GUTIÉRREZ, C., *El hecho ilícito internacional*, Dykinson, 2005, p. 127.

serious violation of rules of *ius cogens*. In addition, it does not allow the invocation of a circumstance that excludes what is illicit to justify such action[432]. In this sense, the ILC recalls that article 21 is a simply reflection of the consensus according to which the self-defence excludes the unlawfulness of one action so long as it is developed according to the UN Charter[433].

As it was pointed out more than half a century ago by De Visscher, "self-defence occupies in the international order a place both essential and poorly defined. Nobody discusses the principle in which it is supported, but its organization through treaties and their concrete applications almost always ends up in a contradiction, either because of the existence of opposing political criteria, or because of the uncertainty arising from the factual circumstances apt to justify his exercise"[434].

According to the International Law, to apply the individual or collective right of self-defence, some requirements are necessary: first, this right can only be exercised in a provisional and subsidiary form in front of the collective security system; second, the main condition is the existence of an armed attack, as expressed under article 51 of the UN Charter; and finally, the right of self-defence must meet three requirements established by customary International Law, which are necessity, proportionality and immediacy.

3. *The role of the UN Security Council in the framework of the collective security system: provisionally and subsidiary*

The conditions which derived from the articulation of the self-defence with the collective security system are specified in article 51 of the UN Charter. In accordance with this article, the action in self-defence is characterized for its *provisionality*[435] (limited in time) and

[432] PELLET, A., "Les articles de la C.D.I. sur la responsabilite de l'Etat pour fait internationalement illicite. Suite-et fin?", *AFDI,* 48, 2002, p. 1-23, at p. 18.

[433] ILC*, "*Draft articles on Responsibility of States...", *op. cit*., vol. ll, part 2, 2001, p. 75.

[434] DE VISSCHER, Ch., *Teorías y realidades en Derecho Internacional Público*, Bosch, 1962, p. 126.

[435] "Until the Security Council has taken measures necessary to maintain international of peace and security" (article 51 of UN Charter).

subsidiarity[436] of the action regarding the UNSC, which is consistent with the primary responsibility attributed to this organ to maintain international peace and security.

Effectively, in the UN Charter, the self-defence is conceived as *provisional*; that is, while the collective defence system of Chapter VII is not effective. Thus, while measures of self-defence begin to take place, States must *immediately inform* the UNSC and determine: if the State has used article 51 correctly and whether it should or should not take collective measures replacing the individual. However, it can also estimate that no collective measure is necessary. The UNSC will unanimously be able to paralyze the actions undertaken. Nevertheless, it has never been done so because it has always been vetoed before having the chance.

Although States, in this regard, do not need authorization of the UNSC, such States must stop their armed responses when the UNSC adopts the "necessary measures" to maintain or restore international peace and security. In fact, it is a way of contributing to ensure compliance with the general prohibition of article 2(4) of the UN Charter.

The obligation to report the UNSC is independent of the correction itself of the acts adopted by States in self-defence. It is a formal obligation expressly provided in the Charter to enable the UNSC to control the use of force allowed by the Charter. The analysis of the fulfilment of this requirement must focus on three aspects: first, the moment when notice must be made. According to article 51, the "measures taken by members in the exercise of this right of self-defence shall be *immediately reported* to the Security Council"[437], duty that has been reiterated by the ICJ in the *Nicaragua case*[438], advisory opinion on the *Legality of nuclear weapons*[439] and in the *Armed activities in the territory of Congo*[440]. Also, the IDI, in

[436] "Measures taken by Members in the exercise of this right of self-defence [...] shall not in any way affect the authority and responsibility of the Security Council […] to take at any time such action as it deems necessary in order to maintain or restore international peace and Security"(article 51).

[437] Italic is ours.

[438] ICJ, *Nicaragua case, op. cit*., par. 200.

[439] ICJ, *Legality of nuclear weapons, op. cit*., par. 44, where the Court affirmed that "Beyond the conditions of necessity and proportionality, article 51 specifically requires that measures taken by States in the exercise of the right of self-defence shall be immediately reported to the Security Council".

its Resolution of 27 October 2007 reaffirmed such duty[441]. Then, the communication of the information will be *immediately reported* after the adoption of the defensive measures, which should not be confused with measures applied; this obligation is not always fulfilled; for example, Iran, after the Iraq attack on 22 September 1980, did not make any communication to the UNSC until 1st October 1980.

Second, the content of the communication to the UNSC. Nothing is needed about the characteristics or the content of the report that States must submit to the UNSC[442]. In practice, the content of the communications are very varied (precise description, or communicate that certain measures have been adopted under the exception of the right of self-defence). The UNSC does not penalize if a State does not realize a precise description, circumstance which deserves criticism because it cannot always determine the nature of the actions.

And third, the consequences of non-compliance with the communication to the UNSC. Initially, the UNSC was more sensitive to this duty, but it has gradually eased the exigency of this requirement (sometimes the information does not reach the UNSC); however, States that claim self-defence tend to give more or less accurate information about their actions.

In any case, it seems excessive to affirm that without carrying out the communication to the UNSC, despite met necessary and proportionate requirements, any immediate act in the right of self-defence becomes illicit. Therefore, the breach of this requirement cannot imply the impossibility to act in self-defence; it would simply represent a violation of procedural duties of States according to article 51 of the UN Charter, since "such a failure is not itself a substantive breach that invalidates the exercise of the right to self-defence"[443].

---

[440] ICJ, *Armed activities in the territory of Congo, op. cit.,* par. 145.

[441] IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., article. 4.

[442] ARAI-TAKAHASHI, Y., "Shifting boundaries of the right of self-defence. Appraising the impact of the September 11 attacks on *ius ad bellum*", The International Lawyer, 36(4), 2002, p. 1081-1102, at p. 1095.

[443] ILA, *Report on aggression and the use of force, op. cit.*, 2016, p. 8; see also, GREIG, D. W., "Self-defence and the Security Council: what does article 51 require?", *ICLQ*, 40(2), 1991, p. 366-402, at p. 366; GREEN, J. A.,

However, the absence of notification may also indirectly affect the generic prohibition of article 2(4). When the UN reserves the monopoly of the control of the use of force in articles 2(6), 2(7), 24, 39, 51, 52, 103, 106 and 108 of the Charter, all States on their own initiative should be interested in demonstrating, in the face of the UN, that its armed acts are in self-defence. According to the ICJ, "it is to be expected that the conditions of the Charter should be respected [...] the absence of a report may be one of the factors indicating whether the State in question was itself convinced that it was acting in self-defence"[444]. Also, the ILA asserts that the "failure to report could support an evidentiary claim that the action was not one of self-defence"[445]. Therefore, the State that does not inform in the right moment, must fight against a very strong presumption facing the self-defence.

Under the right of self-defence, the reaction of a victim State would be fulfilled as soon as the aggressor State's armed attack, in the sense of article 51 of UN Charter, was neutralized, the aggressor State withdrew, or the UNSC adopted the necessary measures. Even though States do not require any authorization of the UNSC to act in self-defence, they all have to refrain from their acts under such right as soon as the UNSC adopts the *necessary measures* to maintain or restore international peace and security.

When is it considered that the UNSC has taken the *necessary measures*? It must be born in mind that the requirement of unanimity between the permanent members of the UNSC can lead to the inactivity of the Council and, therefore, to the continuation of the conflict aside from the institutional action of the UN.

In consideration of the doctrine, there are divergent views on the duration of the action in self-defence. Dinstein asserts that the right of self-defence only extinguishes when the UNSC adopts authentic mandatory decisions in accordance with article 25 of the Charter[446].

"The article 51 reporting requirement for self-defence actions", *Virginia Journal of International Law*, 55(3), 2015, p. 563-625, at p. 592; CERVELL, M. J., *La legítima defensa..., op. cit.,* p. 143-144; and GRAY, C., *International* Law*..., op. cit*., p. 128.

[444] ICJ, *Nicaragua case*, *op. cit*., par. 200

[445] ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 8.

[446] DINSTEIN, Y, *War, aggression..., op. cit*., p. 257.

Instead, some authors mentioned that the State can use force in its defence until there is an unequivocal intention of the UNSC to maintain international peace and security[447]. In fact, in any case, the right of self-defence can continue until the UNSC has taken the necessary measures to maintain international peace and security within the framework of the Chapter VII[448].

The practice of the UNSC is very varied and sometimes the States acted because they were not satisfied with the measures taken by the UNSC (for instance, the UK, that in the case of the Falklands, it was not satisfied with the measures taken by the UNSC in Resolution 502[449] and exercised its right of self-defence). There are other times that States refused to abandon their defensive action, claiming their dissatisfaction with the UNSC ability to replace their individual actions (for example, Iran refusal to accept the Resolution 598 of the UNSC[450] and did not abandon its defensive action).

In addition, there are cases where the UNSC itself does not intend to end an action on self-defence, when it appreciates its necessity and, even, adopting measures of Chapter VII, encourages the continuation of defensive action. In other words, the UNSC in a pragmatic view, accepts implicitly the role of the States to maintain international peace and security when they resort to the right of self-defence[451].

This practice has led some authors to affirm that the self-defence that serves the maintenance of the States must prevail over any other action of the UN, except for the one that, by performing the UNSC operations of force, effectively defends the State (autonomy of self-defence). The action of self-defence, aimed at maintaining international peace and

[447] SONNENFELD, R., *Resolutions of the United Nations Security Council*, Martinus Nijhoff, 1988, p. 124.

[448] KUNZ, J. L., "Individual and collective...", *op. cit.*, p. 879.

[449] UNSC, Resolution 502 on Falkland Islands (Malvinas), 3 April 1982.

[450] UNSC, Resolution 598 on Iraq-Islamic Republic of Iran, 20 July 1987.

[451] See, for instance, BOWETT, D. W., *Self-defence..., op. cit.*, p. 196.

security, is not subordinate to any resolution of the UNSC that does not offer guarantees for the integrity of the State[452].

The subsidiarity does not exclude the UNSC from adopting measures that are developed simultaneously to self-defence[453]; for instance, in the Gulf conflict (1990-1991) where the UNSC adopted a staggered set of measures based on the Chapter VII since the invasion of Kuwait[454]. If Kuwait (and other States) had repelled the invasion and occupation, should have stopped the action on 2nd August, when the Resolution 660 was approved? Or on 29th November when the Resolution 678 was adopted?

The doctrine points out that it would be desirable that the UNSC indicated, at the moment of taking its measures, the conditions in which the State in question has the right to continue using the armed force[455]. In any case, logic leads to the fact that, once the self-defence has begun, it will only be paralyzed if the objective of repelling the attack is achieved or when the military measures of the UNSC effectively facilitate the defence of a victim State. It is necessary to point out, on the one hand, that if the action in self-defence were to cease for the protection of its territory at the moment when the UNSC adopted decisions on Chapter VII, it would invalidate the sense of self-defence[456].

On the other hand, if aggression occurs and the self-defence is not exercised, it is not reasonable for a victim State that has requested the intervention of the UNSC to solve the crisis, to try to invoke its right, unless the effects of the aggression remain and the UNSC action is not feasible due to the veto of one of the permanent members[457].

---

[452] ORTEGA, M. C., *La legítima defensa del territorio del Estado: requisitos para su ejercicio*, Tecnos, 1991, p. 176-177.

[453] CASANOVAS, O., "El principio…", *op. cit*, p. 1076.

[454] UNSC, Resolutions 660, 661 and 678 in 1990.

[455] IDI, "Present problems of the use of armed force in International Law. Humanitarian action", Tenth Commission, 27 October 2007, *Annuaire de l'Institut de Droit International*, vol. 72, 2007, p. 270; and REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 681.

[456] REMIRO, A., *et al*., *Derecho Internacional, op. cit*., p. 681.

[457] *Ibid.*

B. **Armed attack as main requirements for the exercise of the right of self-defence**

1. *Different interpretations of armed attack in the context of the right of self-defence*

Interpretations on article 51 of the UN Charter basically fall in two categories[458]. The first approach is related to a restrictive view of scholarship, jurisprudence and governmental policies that support article 51 as plain terms. The second view corresponds to scholarship and government policies which, based on customary law, advocate expanding the right of self-defence beyond article 51 of the UN Charter. However, interpretations are placed in two categories and have various labels, commonly known as "strict" (restrictive) *versus* "broad" (extensive) view[459].

The *extensive* interpretation, which is the minority, and is supported by authors of interventionist States, points out that self-defence is a legal mean of protection, not only the right to not be a victim of an armed attack, but also other certain essentials rights[460]. In this sense, according to Bowett "action undertaken for the purpose of, and limited to, the defence of a State's political independence, territorial integrity, the lives or property of its nationals cannot by definition involve a threat or use of force"[461]. Bowett also affirms that, although it is generally admitted that article 51 of the UN Charter collects the content of self-defence, it can be argued that customary law of self-defence remains in force by the member States of the Organization. The author asserts that "we must presuppose that rights formerly belonging to member status continue except in so far as obligations inconsistent with those existing rights are assumed under Charter […]. It is, therefore, fallacious to assume that members have only those rights which the Charter accords to

[458] See MORI, T., *Origins of the right of self-defence in International Law. From the Caroline incident to the United Nations Charter*, Brill, 2018, p. 5-6.

[459] See CORTEN, O., "The controversies over the customary prohibition on the use of force: a methodological debate", *EJIL*, 16 (5), 2005, p. 803-822, at p. 804.

[460] WALDOCK, C. H. M., "The regulation...", *op. cit.*, p. 495-515; and SCHWEBEL, S. M., "Aggression...", *op. cit.*, p. 479-497.

[461] BOWETT, D. W., *Self-defense..., op. cit.,* p. 185-186.

them; on the contrary they have those rights which general International Law accords to them except and in so far as they have surrendered them under the Charter"[462].

Therefore, in a broad sense, the self-defence may be exercised when armed force or non-armed force violate the right to territorial integrity, the right to political independence, the right to the protection of citizens, and some rights of economic nature. It should be noted that economic or ideological aggression can be as dangerous as the threat or use of force. Bowett asserted that, in the absence of "any centralized machinery for enforcement of the law", the need for greater self-help is "obvious"[463]. This approach is followed by some governments, especially by military and strong States. These scholars claim that "the every crossing of the Utopian frontier by Arcadian military formations-when this is not authorized by Utopia- constitutes by itself an armed attack, even if no fire is opened at the time of the border-crossing"[464].

The *restrictive* approach demonstrates that only a restricted interpretation of the UN Charter rules is reasonable. According to this position, the restrictive interpretation is more compatible with the contemporary development of the right of use of force by States, which is supported by the UN and the majority of its members. Also, the ICJ stated in the *Nicaragua case* that "for one State to use force against another, on the ground that that State has committed a wrongful act of force against a third State, is regarded as lawful, by way of exception, only when the wrongful act provoking the response was an armed attack"[465]. Furthermore, this view was reaffirmed by the *Eritrea Ethiopia Claims Commission*, declaring that

> "As the text of article 51 of the Charter makes clear, the predicate for a valid claim of self-defence under the Charter is that the party resorting to force has been subjected to an armed attack. Localized border encounters between

[462] *Ibid*, p. 184-185.

[463] *Ibid*, p. 3.

[464] DINSTEIN, Y., *War, aggression…, op. cit.,* p. 213.

[465] ICJ, *Nicaragua case*, *op. cit*., par. 211.

small infantry units, even those involving the loss of life, do not constitute an armed attack for purposes of the Charter" [466].

Hence, in accordance with the limitations set forth in articles 2(4) and 51 of the UN Charter, States can only act in self-defence against an *armed attack*[467]. This way it prevents article 51 from limiting the content of article 2(4) and opens a crackdown on past times where the States determined whether they had or not the right to protect themselves through the use of force. In addition, article 51 is an exception and, therefore, the right of self-defence must be interpreted restrictively.

Thus, article 51 refers exclusively to the self-defence against an armed attack. In this sense, Pellet emphasized that self-defence of article 21 of the 2001 ILC Draft articles of the ILC on responsibility of the State and article 51 of the UN Charter, are only conceived as a response to an armed attack[468].

In addition, this interpretation is compatible with the preparatory works of the UN Charter. In this regard, it should be remembered that the US proposal on 12th May 1945 only referred to the right to self-defence against an aggression or an armed attack. Similarly, a British proposal that tended to extend the scope of the self-defence to any controversy that supposed a rupture of peace was not accepted. Also, the text proposed by the former Soviet Union recognized the self-defence only against an armed attack[469].

---

[466] ERITREA ETHIOPIA CLAIMS COMMISSION, Partial Award, *jus Ad Bellum*, Ethiopia's Claims 1-8, (Ethiopia *v.* Eritrea), judgment of 19 December 2005*, RIAA*, XXVI, par. 11.

[467] CASANOVAS, O., "El principio...", *op. cit.*, p. 1074; CORTEN, O., *The law against war...*, *op. cit.*, p. 126; PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 664; and REMIRO, A., *et al*., *Derecho Internacional, op. cit*., p. 673.

[468] PELLET, A., "Les articles...", *op. cit*., p. 18.

[469] *Foreign Relations of the United States: Diplomatic Papers, 1945, General: The United Nations,* vol. I, 12 May 1945.

2. *Armed attack by States*

As mentioned, article 51 of the UN Charter refers exclusively to self-defence against an armed attack. In other words, an *armed attack* is the prerequisite for a State to resort to the right of self-defence[470]. However, it arises the question of what does armed attack mean and what is the nature of the armed attack to justify the right of self-defence.

By establishing that the classification of an act of aggression corresponds to the UNSC decision, an armed attack must be "sufficiently serious" to justify the self-defence, and by prohibiting the use of force in very broad terms, it is clear that this is a source of problems of interpretation. Although, in practice, the concepts of *use of force* of article 2(4), *aggression* of article 39 as a condition for the adoption of collective measures provided in the Chapter VII or *armed attack* of article 51 as presuppositions of the right to self-defence, are used as equivalent concepts, they do not always coincide.

Article 51 of the UN Charter does not provide elements to determine the concept of armed attack and the adoption of UNGA Resolution 3314 (XXIX) was a significant indirect attempt. However, the definition of aggression contained therein "only claims to specify the notion of 'act of aggression' as it is embodied in article 39 of the Charter, and not that of 'armed attack' as used in article 51"[471]. Also, distinction between *acts of aggression* and *armed attack* were explicitly expressed by the USSR and US[472]. Hence, the notion of *armed attack* and *act of aggression* do not necessarily coincide completely, and the armed attack is the narrowest concept[473] (see Figure 2). However, "the difference between the two is so small

[470] OKIMOTO, C., "The cumulative requirements of *jus ad bellum* and *jus in bello* in the context of self-defence", *Chinese Journal of International Law,* 11, 2012, p. 45-75, at p. 60.

[471] NOLTE, G.; RANDELZHOFER, A., "Article 51", in SIMMA, B.; *et. al*., (eds.), *The Charter of the United Nations: a commentary,* vol. 2, 3rd ed., OUP, 2012, p. 1397-1428, at p. 1407; see also RUYS, T., *'Armed attack'..., op. cit.,* p. 136; and CORTEN, O., *The law against war..., op. cit*., p. 404.

[472] See "Summary Records of the 105th Meeting", UNGA, Doc. A/AC.134/SR.105, 9 May 1973.

[473] The Draft definition submitted to the Special Committee by thirteen Non-aligned countries emphasized in par. 2 of its Preamble that "that armed attack (armed aggression) is the most serious forms of aggression", UN, Doc. A/AC.134/L.16 and Add. 1, 2, 24 March 1969; see also NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1407; BOWETT, D. W., *Self-defence op. cit.,* p. 192; CERVELL, M. J., *La legítima defensa..., op. cit*., p. 81; GRAY, C., *International Law..., op. cit.,* p. 137-138; or DINSTEIN, Y., *War, aggression..., op. cit*., p. 224, among others.

that it is often overlooked"[474]. An armed attack only occurs when the force is used on a relatively large scale with sufficient gravity to have substantial effects[475]. Thus, the UNGA Resolution 3314 (XXIX) does not particularly define the meaning of armed attack and the ICJ only refers to this Resolution in some cases [476].

According to the UNGA Resolution 3314(XXIX), "the first use of armed force by a State in contravention of the Charter" constitutes "*prima facie* evidence, of an act of aggression" (article 2). In article 3(g), the Resolution enumerates a list of classical assumptions which provides direct and indirect aggression with sufficient gravity, which in fact gives useful indications on how to interpret the term *armed attack*[477] (see Figure 1). But, as mentioned *supra*, "the definition includes acts that do not necessarily all qualify as 'armed attacks'"[478]. Then, such list of acts of aggression, subject to certain qualifications, can be characterized as an 'armed attack' within the meaning of article 51[479].

In this context, the ICJ refers to article 3(g) as a possible form of armed attack[480]. Moreover, as it has been seen, the Court distinguishes "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms", implicitly indicating that the mere use of force or acts of aggression by one State against another State in lack of sufficient gravity (the most grave forms of force), can not constitute an armed attack to justify the right of self-defence[481]. In the same direction, *IDI 10A Resolution* mentions that "An armed attack triggering right of self-defence must be of a certain degree of gravity. Acts

---

[474] DAILLIER, P., *et al., Droit International Public,* 8th ed., LGDJ, 2009, p. 1039.

[475] ICJ, *Nicaragua case, op. cit*., par. 191; ICJ, *oil platform case*, *op. cit*., pars. 51, 64, and 72; GREEN, J. A., *The International Court of Justice and self-defence in International Law*, Bloomsbury, 2009, p. 31.

[476] ICJ, *Nicaragua case, op. cit*., par. 195; and, *Armed activities on the territory of the Congo, op. cit.,* par. 146.

[477] NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1410; GRAY, C., *International law…, op. cit*., p. 137 and 146; DINSTEIN, Y., *War, aggression …, op. cit*., p. 209; CORTEN, O., "The controversies…", *op. cit*., p. 404; and RUYS, '*Armed attack'…, op. cit*., p. 139 and 539.

[478] ILC, "State responsibility for international wrongful acts", *op. cit.,* vol. II, part 2, 1980, p. 68.

[479] NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1410.

[480] ICJ, *Nicaragua case*, *op. cit*., par. 195.

[481] *Ibid*, par. 191.

involving the use of force of lesser intensity may give rise to countermeasures in conformity with International Law"[482].

Likewise, the Court in the framework of customary International Law, affirmed that in individual and collective right of self-defence "the exercise of this right is subject to the State concerned having been the victim of an armed attack" and considered that there exists a "general agreement on the nature of the acts which can be treated as constituting armed attacks"[483]. However, this statement is surprising in the view of the unsuccessful previous effort towards agreeing on the definition of armed attack that has not led the ICJ to provide a specific definition of armed attack. Instead, the ICJ just gave one example in order to illustrate the existence of an armed attack in a specific situation and stipulated that the participation of a State in the use of force by an irregular armed band, as described in article 3(g) of the UNGA Resolution 3314 (XXIX)[484].

Finally, to constitute an armed attack, intention of offender to harm a specific target of a victim State is noticeable. According to the ICJ judgment in the *Oil platform case*, an armed attack must be carried out "[…] with the specific intention of harming" a particular State[485]; albeit, this view of the ICJ has been criticized by some institution[486].

Now we must cope with the question of whether it is possible or not that an armed attack occurs within the territory of the aggressor State, issue that attract a vast amount of academic debates.

Traditionally, in order to justify the right of self-defence, an armed attack must occurs in an inter-State conflict. In other words, an armed attack shall be directed from outside the

---

[482] IDI, 10A Resolution "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., article 5.

[483] ICJ, *Nicaragua case*, *op. cit*., par. 195; and *Oil Platforms case, op. cit*., par. 51.

[484] See NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1408; ICJ, *Nicaragua case*, *op. cit*., par. 195; and *Oil Platforms case, op. cit.,* par. 146.

[485] ICJ, *Oil Platforms case, op. cit.,* par. 64.

[486] For instance, see *The Chatham House principles..., op. cit.,* p. 966.

territory controlled by a victim State[487]. To constitute an armed attack, the security or existence of a State must be under threat. Hence, an attack to nationals abroad or any attack that does not threaten the security or existence of a State cannot, according to most of the commentators, constitute an armed attack[488].

However, the ICJ, in the case of *Tehran Diplomatic staff* in 1980, used the phrase *armed attack* when discussing about seizure of the US embassy staff as hostages by Iranian militants in November 1979[489]. Therefore, the US response was under the right of self-defence[490]. In this sense, some scholars refer that an armed attack on the right of self-defence cannot only be limited to the territory of another State. They emphasised that any use of force against State installations, such as military bases or embassies in the territory of the aggressor State may constitute an armed attack and a victim State is entitled to exercise the right of self-defence[491]. Then, they assert that the *de-territorialisation* of the armed attack concept is not incompatible with the nature of the right of self-defence to protect nationals abroad *per se*[492]. Also, this approach is followed by the *Chatham House* that affirms that

> "the armed attack may include not only an attack against a State territory, but also against emanations of State such as embassies and armed forces. An

[487] ICJ, *The wall, op. cit,* par. 139; see OKIMOTO, C., "The cumulative requirements...", *op. cit.,* par. 38, p. 60.

[488] RONZITTI, N., *Rescuing nationals abroad through military coercion and intervention on grounds of humanity*, Martinus Nijhoff, 1985, p. 11; see also HENKIN, L., *How nations behave: law and foreign policy*, CUP, 1979. p. 141-145; ZEDALIS, R. J., "Protection of nationals abroad: is consent the basis of legal obligation?", *Texas International Law Journal*, 25, 1990, p. 209-270, at p. 238; AZUBUIKE, E. Ch., "Proving the scope of self-defence in International Law", *Annual Survey of International and Comparative Law*, 17(1), 2011, p. 129-183, at p. 159-160; RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 226; or NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1413.

[489] ICJ, *case of consular staff in Tehran, op. cit.,* pars. 56-68.

[490] DINSTEIN, Y., *War, aggression…*, *op. cit*, p. 216.

[491] *Ibid*, p. 214; BOWETT, D. W., *Self-defense..., op. cit.,* p. 91-94.

[492] HENDRICKSON, R. C., "Article 51 and the Clinton Presidency: military strikes and the UN Charter", *Boston University International Law Journal,* 19, 2001, p. 207-245, at p. 214.

armed attack may also include, in certain circumstances, attacks against private citizens abroad or civil ships and airlines"[493].

Thus, according to this extensive approach, based on emanations of a State, an armed attack can be constituted by invasion outside the territory of a State, such as the attack to warships on the high seas or the destruction of military satellites of another State in the outer space. In order to justify this position, they refer to the ICJ's view where "The Court does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'"[494]. In this sense, even the use of force against the embassy of a State within the territory of a third State, can constitute an armed attack that allow to resort to the right of self-defence; in this regard, they refer to the reaction of international community to the US strikes in relation to the destructive bombing of the US embassies in Kenya and Tanzania in 1998 while a few States denounced the US strike[495]. Therefore, based on this extensive point of view of armed attack, there is no need for territorial nexus[496].

Furthermore, ILA in relation to the extensive nature of the principle of the prohibition of the threat or use of force asserts that "there may be room to describe certain rescue operations as not consisting of use of force"[497]. In this regard, the ILA, by reliance on the necessity criteria as primary priority to justify these operations, posed some preconditions: i) the sending State does not engage in any hostilities; ii) there must at least an attempt to seek permission, and iii) the territorial State does not actively object to the evacuation operations[498]. Such operations would be more justifiable if it was clear that nationals had

---

[493] *The Chatham House principles*…, *op. cit*., p. 965.

[494] ICJ, *Oil Platform case, op. cit*., par. 72.

[495] DINSTEIN, Y., *War, aggression…, op. cit.*, p. 217; see also VITKOWSKY, V. J., "Remarks on customary International Law and the use of force against terrorists and rogue State collaborators", *ILSA Journal of International and Comparative Law*, 13(2), 2007, p. 371-378, at p. 374-375.

[496] RUYS, T., *'Armed attack'...,* p. 32-34; and SCHACHTER, O., "The right of States...", *op. cit*., p. 1632.

[497] ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 13.

[498] *Ibid;* see also IIFFMCG that emphasised that "such actions should be limited in scope and duration and exclusively focused on rescuing and evacuating nationals", IIFFMCG, *Report on the conflict in Georgia*, vol. I, September 2009, p. 24-25.

been attacked directly because of their nationality and are seen by their attacker as individual manifestations of their State[499].

Despite this extensive view, any armed action to rescue nationals abroad cannot be justified based on the right of self-defence because the territorial element is necessary to constitute an armed attack in the sense of the right of self-defence. Then, given that it lacks the armed attack requirement, its resort to the right of self-defence is not lawful[500]. Also, the necessity requirement for the justification of the right of self-defence cannot exist in such protective measures[501].

Nevertheless, it is necessary to point out that the ICJ in *Tehran Diplomatic staff* just briefly mentioned but did not address the substance of the issue[502]. Then, the international response shows a clear division between States, where there are a few States that accept the legal right to protect national abroad. In this sense, the positions of the US, the UK, Israel and Belgium in favour of such wide right of self-defence have attracted little support[503]. Therefore, in accordance with most of the States view, diplomatic missions and individual citizens abroad cannot be object of an armed attack in the context of the right of self-defence[504]. Also, article 3(d) of UNGA Resolution (XXIX), in order to define acts of aggression did not include the attack to the nationals abroad as example of acts of aggression. It seems that the extensive interpretation of armed attack gives rise to the blurring of the contours of right of self-defence[505].

---

[499] DINSTEIN, Y., *War, aggression…, op. cit*., 275.

[500] See GRAY, Ch., *International Law..., op. cit*., p. 134; and NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit.,* p. 1401-1403.

[501] RABY, J., "The State of necessity and the use of force to protect Nationals", *Canadian Yearbook of International Law*, 26, 1989, p. 253-272; see also ILC "State responsibility", Documents of the thirty-second session, *Yearbook of ILC*, vol. II, part 1, 1980, article 33.

[502] See NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1413; and ICJ, *case of consular staff in Tehran, op. cit*., pars. 32, 93 and 94.

[503] See GRAY, Ch., *International Law..., op. cit*., p. 166.

[504] GAZZINI, T., *The changing rules on the use of force in International Law*, Manchester University Press, 2005, p. 171; CORTEN, O., *The law against war…, op. cit.*, p. 404 and 510; see also RUYS, T., "The protection of nationals doctrine revisited", *JCSL*, 13, 2008, p. 233-271, at p. 258-260.

[505] See NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1413.

In addition to that, the ICJ, in the *Wall,* rejected Israel's argument that the construction of the wall was a reaction under the right of self-defence. In fact, the Court declared that building the wall in response to armed attacks by Palestinian which originated from territory under control of Israel, cannot be justified under the right of self-defence[506]. Thus, the attack must come from the territory of another State.

Furthermore, in 2000 in the ILC, Dugard, the Special Rapporteur on diplomatic protection, proposed an article allowing military actions to protect nationals abroad under specific circumstances[507], but the harsh criticisms generated among their colleagues and by the States motivated their withdrawal[508].

Theoretically, forcible operations by States to rescue their own nationals abroad is not accepted to justify the exercise of the right of self-defence; however, some State practice on protection of nationals abroad has been developed at least since 1960[509]. In this context, a well-known example are the UK military operations in Suez in 1956; Mayaguez incident in 1975; the freeing of hostages by Israel at Entebbe in 1976; US military operation to free its diplomatic staff held hostage in Iran in 1980; landing of US troops in Granada on October 1983; US military intervention in Panama in December 1989; US operation in Libya in 1990; France and US actions in Central African Republic in 1996 and 2003, Belgium and France in Rwanda in 1990, 1993 and 1997; France in Chad in 1992 and 2006, Germany in Albania in 1997 or France in the Ivory Coast in 2002-2003[510]. In all these circumstances, interferer States asserted that the rescue of nationals abroad is exceptional to justify the right of self-defence, when its nationals abroad lives or health are endangered and a foreign State is unable or unwilling to carry out the required rescue. In addition, these operations confronted inaction from other States and international community[511]. Actually, it seems

[506] ICJ, *The Wall case, op. cit.,* par. 139.

[507] ILC, *First Report on Diplomatic Protection*, 7 March 2000, UN, Doc. A/CN.4/506, pars. 46-60.

[508] RUYS, T., *'Armed attack'…, op. cit*., p. 237-239.

[509] RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 226.

[510] See *Ibid*, p. 227.

[511] For example, several European States expressed their satisfaction in regard to the Israel operation at Entebbe.

there is an over justification allowing limited forcible actions necessary[512] to rescue a State's own nationals abroad if the lives of such nationals are genuinely in danger and the foreign State is unable or unwilling to ensure safety of their nationals. Then, intervention does not follow any other purpose and the scale and effects of rescue operations are proportionate with minimum damage to the territory of another State[513].

Although such rescue operations have been tolerated by international community due to the special circumstances involving the situation[514], it seems it is no longer possible to support the extensive approach to exercise the right of self-defence in these cases, because it opens the window to abuse of such right as a pretext for the intervention in the territory of another State, for instance, to assemble a new government[515].

During the latest years, States have invoked in few cases the protection of their nationals for actions in self-defence, mainly because they seek other justifications. Thus, it is not possible to talk about a generalized practice. However, the appearance of the *Daesh*, has provided States with a new opportunity to think again about the right of defence for the protection of their nationals abroad[516].

Another interesting question is the *trigger of armed attack beyond first shot*. In several circumstances, hostile States accuse each other to initiate an armed attack; hence it is important to determine the moment where an armed attack begins. The simplest criteria is the *first shot*; in accordance with article 2 of the UNGA Resolution 3314 (XXVX) "the first use of armed force by a State in contravention of the Charter is a *prima facie* evidence of aggression" and may constitute an armed attack. This Resolution, under article 3(c) mentions that "the blockade of the ports or coasts of a State by the armed forces of another

[512] See GRAY, Ch., *International Law..., op. cit*., p. 166-169, where asserts that among others "only the rescue operation of the Mayaguez, and those in Iran and Entebbe were limited actions".

[513] See BOWETT, D. W., *Self-defence..., op. cit.,* p. 44; and RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", *op. cit*., p. 228.

[514] See GAZZINI, T., *The changing rules on the use of force..., op. cit.,* p. 170-171.

[515] RUYS, T., "The protection of nationals..., *op. cit*., p. 261.

[516] See CERVELL, M. J., *La legítima defensa*…, *op. cit*., p. 263-264.

State" can constitute an act of aggression if occurs effectively[517]; in this case, an aggression can be an armed attack without the first shot. In this kind of acts of aggression, the majority of States are reluctant to consider it an obstruction of transit across land to the open sea as an armed attack[518]. However, this form can be acceptable especially in extreme situations if the blocking effects are equivalent to military invasion, such as cutting off all communication routes[519].

Moreover, in conformity with article 3(e) of such Resolution, "the use of armed forces of one State which are within the territory of other State with agreement of the receiving State, in contravention of the conditions provided in the agreement or any extension of their presence in such territory beyond the termination of the agreement", may constitute an armed attack even without shooting fire, and territorial States in this case are justified to use force in the right of self-defence[520]. For instance, in the issue of the withdrawal of consent by the DRC when "the DRC accused Rwanda and Uganda of invading its territory", it claimed that "any earlier consent by the DRC to presence of Uganda troops on its territory had at latest been withdrawn by 8 August 1998". In this regard, the ICJ "recalls that, independently from the conflicting views as to when Congolese consent to the presence of Ugandan troops might have been withdrawn, the DRC informed the Court that its claims against Uganda began with what it terms an aggression commencing on 2 August 1998"[521]. Thus, the presence of military force in territory of other State over the previous agreement can constitute an aggression.

Also, one State may use the force in self-defence even before its territory is penetrated by military force when one State launches an Intercontinental Ballistic Missile (ICBM) and a few minutes prior to impact, radar network of State immediately detected and used the

[517] NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1410-1411; RUYS, T., *'Armed Attack'…, op. cit.,* p. 267; and CONSTANTINOU, A., *The right of self-defence under customary International Law and article 51 of the United Nations Charter*, Diss. University of Nottingham, 1996, p. 76-81.

[518] See CONSTANTINOU, A., *The right of self-defence…, op. cit.,* p. 81.

[519] NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1410-1411.

[520] GRAY, C., "The Eritrea/Ethiopia Claims Commission oversteps its boundaries: a partial award?", *EJIL*, 17(4), 2006, p. 717; and DINSTEIN, Y., *The war, aggression…, op. cit*., p. 229-230.

[521] ICJ, *Armed activities in territory of Congo, op. cit*., pars. 53-54.

force under the right of self-defence; therefore, in this case the *first shot* criteria is not a convenient reason to recognize the offender State[522].

3. *Armed attack by non-State actors, even where no State is substantially involved*

In this section, we are going to answer whether only the States can be victims or authors of an armed attack. The qualification as a victim of a State may give rise to problems in separation processes, particularly when the original State does not recognize the new State. Third States, in relation to the new State, can use the recognition to change its intervention (unlawful) to collective self-defence (lawful), considering it as an aggressor to the State that believes that is fulfilling its constitutional mission in accordance with the right of self-defence to protect its territorial integrity.

Regarding the authors of an armed attack, the possibility of using force in self-defence against the armed attacks of some non-State actors (irregular forces or terrorist groups) is a very controversial issue. Traditionally, a reductionist conception has prevailed, based on the primary and plenary condition of international subjectivity of the sovereign State and in fact that only States are territorial subjects. In fact, the exercise of self-defence against an armed attack just by non-State actors has never been recognized by the ICJ.

The ICJ in its advisory opinion on the *Wall* interpreted article 51 of the UN Charter in a restrictive view, affirming that such article "recognizes the existence of an inherent right of self-defence in the case of an armed attack by one State against other State"[523]. The Court rejected the invocation to self-defence by Israel, *inter alia*, since Israel response in the *Occupied Palestinian Territory* would not be attributable to a foreign State; otherwise its origin would be in armed groups that acted within the territory Israel occupied militarily[524].

[522] DINSTEIN, Y., The *war, aggression…, op. cit.,* p. 230.

[523] ICJ, *The Wall*, *op. cit*., par. 139.

[524] *Ibid*, par. 139.

Therefore, some scholars emphasized on the ICJ view in the *Wall,* claiming that the Court was reluctant to accept the right of self-defence against non-State actors[525]. Therefore, there is a fundamental problem of non-State actors since they reside in a territory under the sovereignty of one State. In this regard, any use of force in the exercise of the right of self-defence in the territory of another State against a non-State actor would violate article 2(4) of the UN Charter, because it would cause a breach of the territorial integrity of host States[526].

The ICJ interpretation in the *Wall* is implicitly reaffirmed in the case of the A*rmed activities on the territory of Congo*, where the Court held that the attack carried out by anti-Ugandan rebels that emanate from DRC territory was not attributable to this State; hence, Uganda did not have the justification to resort to the right of self-defence against DRC[527]. According to the ICJ view, it is clear that the Court has a strict approach on the use of the right of self-defence since "article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters"[528].

The ICJ explanation of the term armed attack refers to the element of *substantial involvement* in the sending of irregular armed groups which is contained in article 3 (g) of the UNGA Resolution 3314 (XXIX), and thereby implies that this conduct also comes within the notion of an armed attack. However, it is necessary to bear in mind that application of the rather vague term *substantial involvement* which allows for variety of value-oriented assessments, requires a particular careful consideration of the rules on the burden of proof, as the Court has demonstrated in *Armed activities on the territory of Congo* judgment[529]. In this case, it refused to respond to the requests of the parties about "if and under what conditions contemporary International Law provides for a right of self-defence against

[525] ICJ, *Armed activities on the territory of Congo*, *op. cit.* par. 146.

[526] COUZIGOU, I., "The fight against…", *op. cit.*, p. 86.

[527] ICJ, A*rmed activities on the territory of Congo*, *op. cit*. par. 146.

[528] *Ibid,* par. 148.

[529] *Ibid*, par. 146; see also NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1415.

large-scale attacks of irregular forces"[530]. It seems that the Court's decision to refuse to answer the question is not a reason to believe that the ICJ absolutely precluded the right of self-defence against non-State actors within the territory of other State[531]. That is, the Court leaves open the same possibility that International Law provides for the right of self-defence against attacks of non-State actors when territorial State is unable or unwilling to prevent such acts by non-State actors from its territory.

Also, this restrictive view of self-defence was evidenced in the UNSC approach. In front of terrorist attacks by the Palestine Liberation Organization (PLO) which was hosted in Tunis, Israel in October 1985 bombed the PLO quarters in Tunis. The UNSC in the Resolution 573 did not admit the Israeli argument of self-defence against the terrorist attack by the PLO and condemned the bombing and even declared that Tunis had "the right to reparation […]"[532].

Contrary to these views, some judges, such as Higgins, Kooijmans and Buergenthal expressed their dissatisfaction with the Court's point of view in their separate opinions. In similar statements, the Judges asserted that nothing in the text of article 51 indicates that self-defence is only available when an armed attack is made by a State[533]. In this sense, some scholars by referring to *Caroline incident* between the US and the Great Britain in 1837, assert that this incident affirmed the applicability of the right of self-defence against armed attacks by non-State actors because the US did not have effective control on that insurgent group[534]. In addition, they claim that article 51, unlike other articles of the UN Charter, such as article 2(4) that specifically refers to States, "does not mention the nature

[530] ICJ, A*rmed activities on the territory of Congo*, *op. cit*., par. 147.

[531] TRAPP, K. N., "Back to basic: necessity, proportionality, and the right of self-defence against non-State terrorist actors", *ICLQ,* 56(1), 2007, p. 141-156, at p. 141-143.

[532] UNSC, Resolution 573 on Israel-Tunisia, 4 October 1985.

[533] ICJ, *The wall, op. cit*., separate opinion of Higgins, par. 33 and Kooijmans, par. 35; and declaration of judge Buergenthal, par. 35; see LUBELL, N., *Extraterritorial use of force against non-State actors*. OUP, 2010, p. 32.

[534] In this case, British-Canadian used of armed force in self-defence against local insurgents who primary tried to capture Toronto, see PAUST, J. J., "Self-defence targeting of non-State actors and permissibility of US use of drones in Pakistan", *Journal of Transnational Law and Policy*, 19(2), 2010, p. 237-279, at p. 243 and 244.

of the party responsible for the attack, but, only that of the entity which has the right of response"[535].

In fact, regarding non-State actors, the problem is how to submit a relationship to International Law when the aggressor lacks legal personality. In addition, these *non-State actors* (individuals or groups, for instance, those that execute terrorist attacks) must have territorial bases which are only offered to States. The tendency is to impute directly (if they are agents of the State itself) or indirectly to host States the possible or supposed aggression of their "guests". To attribute the acts of a non-State actor to a State is unquestionable if there is evidence that the author of such act was a State organ acting in its capacity[536].

The indirect operations (by non-organ or agents of the State) when State sponsors non-State actors in one form or more (for instance offering finance assistance, providing logical support and know-how, or facilitating bases and training fields), all these behaviours are prohibited by International Law. According to UNGA, Resolutions 2625 (XXV), 2734 (XXV)[537], and 3314 (XXIX), all States have the duty to refrain from organizing, instigating and supporting terrorist acts executed in another State or participating in them, and allow them to organize activities in their territory aimed to the commission of such acts, and this has been reiterated by the UNSC, by invoking the UNGA Resolution 2625 (XXV), in Resolutions 1189 (1998)[538], and 1373 (2001), among others.

A State that provides assistance to individual or terrorist groups, is not easy to impute such acts to this State (unless it is done by its organs or agents). In this sense, in the *Nicaragua case*, the ICJ affirmed that the various forms of assistance to the *Contra* were not sufficient to demonstrate complete affiliation to the US. Consequently, in order to attribute the

[535] LUBELL, N., *Extraterritorial ..., op. cit.,* p. 31-32.

[536] CONDORELLI, L., "The imputability to States of acts of international terrorism", *Israel Yearbook on Human Rights*, 1989, p. 233-246, at p. 233-234.

[537] UNGA Resolution 2734 (XXV) "Declaration on the Strengthening of International Security", 16 December 1970.

[538] UNSC, Resolution 1189 on the international terrorism, 13 August 1998.

military and paramilitary activities by the *Contra* in Nicaragua to the US, the *effective control* of the operations by the US must have been proven[539].

Even applying this criterion to the complicity of the Taliban regime with Al-Qaeda, this would not have been sufficient to sustain the legality of the self-defence of the armed action by the US, with the UK support, against Afghanistan[540]. In order to impute events of 11 September 2001 to Afghanistan government, it was necessary to prove the *effective control* of the Taliban regime on Al-Qaeda[541]. In addition, the fact that the Taliban were not recognized as the legitimate government by the UN and most of its members, still adds more problems to impute to Afghanistan. However, all these do not prevent the attribution to the Taliban of the responsibility for what they were accused of in the territory under their control[542]. In this sense, it is normal for the UNSC that directly mandates and imposes sanctions in these cases; for instance, Resolution 913 (1994) and 1034 (1995) which addressed the Serbian faction in Bosnia and Herzegovina; Resolutions 811, 823, 834, and 851 of 1993, 1127 (1997), and 1237 (1999) to UNITA (Angola); or the Resolution 1071 (1996) to the Somalia factions.

In any case, it is clear that something is changing since the movements or armed groups that use the force against a State are increasingly stronger and States lose their control on their own territories, such as Al-Qaeda in Afghanistan. Thus, some States, doctrines and judges have argued that the limitation of the use of self-defence among States, is not a requirement of article 51 of the UN Charter but it is a result of a traditional and restrictive interpretation. In this regard, it is necessary to adopt an open position to accept that the

---

539 ICJ, *Nicaragua case, op. cit*., par. 115.

540 O'CONNEL, M. E., "Lawful self-defense to terrorism", *University of Pittsburgh Law Review*, 63, 2002, p. 889-908, p. 901-902.

541 BYERS, M., "The intervention in Afghanistan-2001", in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 626-638, at p. 633; see also CORTEN, O., Regulating resort to force: a response to Mathew Waxman from a "Bright Liner", *EJIL*, 24, 2013, p. 191-197, at p. 195.

542 ILC, "Draft articles on responsibility of States", *op. cit*., vol. II, part 2, 2001, article 10.

right of self-defence can cover the reaction against an armed attack by a non-State actor which is not subject of International Law[543].

Consequently, in addition to resorting to the self-defence in the case of armed attack by non-State actors, following *effective control* test, two more cases have been accepted: firstly, if an armed attack is launched from a space beyond any State's jurisdiction[544]; and secondly (and also the most problematic case-scenario), when the armed attack has been carried out from the territory of another State that does not have the ability to exercise territorial control[545].

In this sense, it seems feasible to subsume the military operations of the US (and its allies) in Afghanistan in response to terrorist attacks attributed to non-State actors (*Al-Qaeda*), with the complicity of unrecognized government (Taliban regime) of a UN State member (Afghanistan)[546].

The premise, on the one hand, is an armed attack; subsequently, we must find out if the non-State actor acts are equivalent to an armed attack by States with high gravity. As it was seen *supra*, the ICJ ruled out that frontier incidents or the support of armed bands and irregular groups below a certain threshold of gravity does not constitute an armed attack under article 51 of the UN Charter. Likewise, the mere supply of findings by the State to the *contras* cannot justify the right of self-defence against another State[547]. In the *Nicaragua case*, the US asserts that Nicaragua had triggered an armed attack against El Salvador and other Central American States, and therefore the US actions against Nicaragua were

---

[543] IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., article 10(i); see also REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 677; and BETHLEHEM, D., "Self-defense against an imminent or actual armed attack by non-State actors", *AJIL*, 106, 2012, p. 770-777.

[544] See ICJ, *Oil Platform case, op. cit*., par. 72; and IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., article 10(ii).

[545] See *Armed activities in the territory of Congo, op. cit*. separate opinion of judges Kooijmans, pars. 28-32; and SIMMA, pars. 4-15; as well as TAMS, C. J., "The use of force against terrorists", *EJIL*, 20(2), 2009, p. 359-397; and REINOLD, T., "State weakness, irregular warfare, and right to self-defense post 9/11", *AJIL*, 105, 2011, p. 244-286.

[546] REMIRO, A., *et al*., *Derecho Internacional*, *op. cit.,* p. 677 and 682.

[547] ICJ, *Nicaragua case, op. cit*., par. 228.

justified on the right of self-defence. The ICJ did not accept these allegations and pointed out that "the Court is unable to consider that, in customary International Law, the provision of arms to the opposition in another State constitutes an armed attack on that State"[548]. It concluded that the US had only violated the principle of prohibition of the threat or use of force[549] .

On the other hand, the action in self-defence will have to be localized on the space under the control of the aggressor and their resources, without extending it (unless it is attributed to the author) to the territory and resources of the State hosting the aggressor.

Now we must find out whether terrorist acts can activate article 51 of the UN Charter. It will have to be assessed if the acts in question (whether made by individuals or groups of people, or by organs or agents of a State "State terrorism") have a sufficient degree of intensity and gravity to be able to be qualified as an armed attack within the meaning of article 51 of the Charter.

As mentioned *supra,* the right of self-defence can be invoked against terrorist groups or irregular mercenaries, despite not being part of the official apparatus of a State, when they really act in name and on behalf of such State, who sets the objectives and eventually instructs, finances or equips this groups, which is equivalent to an indirect attribution of the acts. Moreover, the right of self-defence can be exercised in front terrorist attacks characterized by the intervention of a State allowing the use of its territory for passage, training or withdrawal of the terrorist group, or by helping in any other way to this group[550].

---

[548] *Ibid,* par. 230.

[549] *Ibid,* par. 123.

[550] SÁNCHEZ, L. I., *Derecho Internacional y crisis internacionales*, Iustel, 2005, p. 186; see also, among others, LOBEL, J. "The use of force to respond to terrorism attacks: the bombing of Sudan and Afganistan", *Yale Journal of International Law*, 1999, p. 537-557; FRANCK, Th. M., "Terrorism and the right of self-defensa", *AJIL*, 95(4), 2001, p. 839-843; REMIRO, A., "Terrorismo, mantenimiento de la paz y nuevo orden", *REDI*, 2001, p. 125-171; ALCAIDE, J., "La guerra contra el terrorismo: ¿una OPA hostil al Derecho de la Comunidad internacional?", *REDI*, 53(1/2), 2001, p. 289-302; and O'CONNELL, M. E., "Lawful self-defense to terrorism", *op. cit.,* p. 889-908.

A complicate matter is to find out whether offering a *sanctuary* to a terrorist group (for instance, Lebanon in 1982, and Tunisia in 1985 to PLO; Afghanistan in 2001 to Al-Qaeda or Lebanon in 2006 to Hezbollah) may be sufficient to justify an armed response. An even more complex problem is when terrorist attacks come from individuals or groups of people acting in territory, outside of the control of any State. In other words, is it possible to activate the self-defence against attacks from *non-state actors*?

It should be remembered that such acts of terrorism must be *international* in nature, directed from the territory of one State against other. In this regard, it is interesting to refer to the construction of the Wall by Israel in the *Occupied Palestinian Territory*. Israel claimed that the Wall was in accordance with article 51 of the Charter, and UNSC Resolutions 1368 and 1373 in 2001. Particularly, Israel indicated that these resolutions recognized the right of self-defence against terrorist acts.

In light of these allegations, as is mentioned *supra*, the ICJ indicated that Israel had not argued that such acts were attributable to a foreign State, since there was no doubt that it exercised control of the Palestinian territory, and the threat that it invoked to justify the construction of the Wall had its origin inside that territory, and not outside of it. Thus, this view indicates that the use of force in the right of self-defence is only applicable against terrorist attacks between States (inter-States), not in cases of internal violence (in the territory of a State or in a territory which is occupied by that State). This does not mean that a State cannot defend, even with self-defence, when other State *send* armed bands or *command* and *effectively control* them; it will only be necessary that such acts to be comparable to their gravity to a genuine armed attack[551].

As we have seen above in the framework of customary International Law on the prohibition of the use of force, the ICJ indicated that there is distinction between the most gravity use of force and others less graves, but made it clear that in the case of self-defence

[551] ICJ, The *Wall*, *op. cit.*, pars. 138-139; see individual critical opinion of judges such as Kooijmans, pars. 35-36, and Higgins, pars. 33-34; as well as MURPHY, S. D., "Self-defence and the Israel Wall advisory opinion; an *ipse dixit* from the ICJ?", *AJIL,* 99(1), 2005, p. 62-76; WEDGWOOD, R., "The ICJ Advisory Opinion on the Israeli...", *op. cit.*, p. 58; and TAMS, C. J., "Light treatment of a complex problem: the law of self-defence in the Wall case", *EJIL*, 16(5), 2005, p. 963-978.

both individual and collective "cannot be exercised more than if the State concerned has been the victim of an armed attack"[552], and considered that there is "general agreement on the nature of acts which can be treated constituting armed attacks", understood as such acts, the actions of some intensity that are not "a mere frontier incident" between regular armed forces"[553]. That is, resorting to the criterion of the scale and effects of hostilities, indicates that not all uses of force can be included in the category of armed attack, only the most grave forms.

In addition, the Court, in relation to simple border incidents, affirmed that such incidents can not constitute armed attack to justify a self-defence response as well as the provision of arms or logistical support to armed bands or irregular groups[554]; the punctual attack with the launch of a missile against a merchant ship; the repeated shots towards a military helicopter from a patrol boat; or the placement of a mine which warship collide[555].

However, the ICJ understands that the armed attack demands by the right of self-defence are given in the cases of *indirect aggression* mentioned in article 3(g) of Resolution 3314 (XXIX); that is, when the armed acts are comparable by their gravity to what was stated in paragraphs a) to f) of such article, and are committed by groups or armed bands that are

[552] ICJ, *Nicaragua case, op. cit*., par. 195, reiterated in *Oil Platforms case, op. cit*., par. 51.

[553] ICJ, *Nicaragua case, op. cit.*, par. 195.

[554] In the *Nicaragua case*, *ibid*, the ICJ against US argument that Nicaragua had triggered an armed attack *versus* El Salvador and other Central American States, and acts of the US against Nicaragua were in self-defence; the ICJ did not accept US allegation and denied that notion of "armed aggression" may also cover "assistance to rebels in the form of the provision of weapons or logistical or other support"(par. 195); and added that "the Court is unable to consider that, in customary International Law, the provision of arms to the opposition in another State constitutes an armed attack on that State" (par. 230); the Court concluded that "the United States has violated the principle prohibiting recourse to the threat or use of force" (par. 238); ICJ, *Nicaragua case, ibid.*

[555] The ICJ in response to the US attack on the Reshadat complex on 19 October, 1987, pointed out that the impact of ship of the US with mine place by Iran, the repeated shots of Iranian boats against helicopters of the US Navy, and the launch of a missile *versus* US Navy, "even taken cumulatively […] these incidents do not seem to the Court to constitute an armed attack on the United States" which in the *Nicaragua case*, the Court described as the "most grave forms" of a use of force and, therefore, did not act in self-defence (par. 64); likewise, the US attacks to other complexes on 18 April 1988, although the ICJ "does not exclude that the possibility that the mining of single military vessel might be sufficient to bring into play the 'inherent right of self-defence'; but in view of all the circumstances […] Court is unable to hold that the attacks on the Salman and Nasr platforms have been shown to have been justifiably made in response to an 'armed attack' on the United States by Iran, in forms of the mining of the USS *Samuel B. Roberts*"(par. 72); ICJ, *Oil Platforms case, op. cit.*

sent by a State or which are substantially involved in such acts. To add, article 3(g) reflects customary International Law[556] .

Can terrorist attacks of 11 September be described as an armed attack in order to accommodate the right of self-defence? Could it be understood that those groups were sent by Afghanistan government or that their attacks were carried out with substantial involvement of such government?

There is no evidence that proves whether the Taliban Government in Afghanistan sent specific instruction to *Al-Qaeda* terrorists or they acted on their behalf. However, the Government offered support and gave refuge to *Al-Qaeda* in its territory, and by doing so this allowed them to build their own training bases and always refused to extradite their leader Osame Ben Laden. Does this mean that Afghanistan had a substantial participation in the events of 11 September? Our answer would be negative. If we take into account the level of control required by the ICJ in the *Nicaragua case*, where it indicated that *effective control* should refer to each specific act, it is not sufficient to impute an attack to Afghanistan even if it provided financial or arm provisions support. In order for the US to assume legal responsibility, as we have seen *supra* "it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed"[557]. In addition, the support of Afghanistan to *Al-Qaeda* was more passive and less vehement than what the US did to the *Contra* in its fight against the Sandinista government of Nicaragua. Thus, it can be confirmed that Afghanistan violated the principle that prohibits the direct or indirect use of armed force,

[556] In *Nicaragua case*, the ICJ notes that "In particular, it may be considered to be agreed that 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"; ICJ, *Nicaragua case*, *op. cit.,* par. 195.

[557] *Ibid*, par. 115; see also pars. 111, 193-195 and 210-211.

but not an indirect aggression, in the sense of article 3(g) of the definition of aggression, against the US, that could generate in its favour the inherent right of self-defence[558].

Dinstein, referring to the lack of *effective control* of *Taliban* on acts of *Al-Qaeda*, concludes that *Al-Qaeda* cannot be regarded as *de facto* organs of Afghanistan. Hence, the right of self-defence in the UNSC Resolution 1368, implicitly indicates that the scope of the right of self–defence is extended to terrorist or armed bands as "horrifying terrorist attacks" without expression of armed attack. In other words, if the right of self-defence is activated in the UNSC Resolutions 1368 and 1373, this inevitably implies that an armed attack is involved[559].

Also, *Chatham House,* after sending questioners to the small groups of International Law academics, asserted that "there is no reason to limit a State's right to protect itself from an attack by another State. The right of self-defence is a right to use force to avert an attack. The source of the attack, whether a State or a non-State actor, is irreverent to the existence of the right"[560]. They claimed that the ICJ in the *Wall* did not affirm that an armed attack cannot be constituted, unless it occurs by States. Likewise, this limitation is not visible in article 51 on the UN Charter. Also, as is mentioned *supra*, these scholars invoked the *Caroline case* where the criteria announced in the field of marauding armed band, not orthodox State-to-State conflict. In addition, they claimed that the UNSC Resolutions 1368 and 1373 of 2001 justify the exercise of the right of self-defence against non-State actors; in this sense, these Resolutions indicate that there is not restriction in the scope of the right of self-defence to the reaction against terrorist groups. Hence, the fighting in Afghanistan in 2001 was a reaction against the *Al-Qaeda* and not *Taliban*[561].

---

[558] See GUTIÉRREZ, C., "El 'uso de la fuerza' en los Informes del Grupo de Alto Nivel (2004), del Secretario General (2005) y, a la postre, en el Documento Final de la Cumbre de Jefes de Estado y de Gobierno (Naciones Unidas, Nueva York, Septiembre de 2005)", *UNISCI Discussion Papers*, 10, 2006, p. 75-100, at p. 88-90.

[559] DINSTEIN, Y., *War, aggression …, op. cit.,* p. 246-247.

[560] *The Chatham House principles…*", *op. cit.,* p. 969.

[561] *Ibid,* p. 970.

Having said that, how can the attacks of the US and the UK to Afghanistan be explained? Is this the beginning of a new concept of self-defence that would accept preventive self-defence? After the aftermath of the events of 11 September 2001, States widely accepted that Stateless and borderless terrorist organizations are a great threat to States and the international community. At first, it should be considered that terrorist attacks on 11 September 2001 have been unanimously condemned by the UNGA in Resolution 56/1 of 2001[562] and by the UNSC Resolutions 1368 and 1373. These, on the one hand, particularly, in the Resolution 1368, it describes acts of terrorism as a threat to international peace and security, and acknowledges, for the first time, that in front of a terrorist attack, the victim State has the "inherent right of individual or collective self-defence in accordance with the Charter". It also admits for first time that a State has the right of self-defence in the case of an armed attack, even if it has not been committed by another State[563]. What in Resolution 1368 were mandatory measures against specific terrorist attacks, in the Resolution 1373 they turned to mandatory measures to combat all types of terrorism. Thus, the recognition of the inherent right of individual or collective self-defence against all kinds of terrorist attack is widespread.

On the other hand, it must be taken into account that the NATO member States (19 who are neither the smallest nor the weakest) have formally considered that the attacks of 11 September could be subsumed in article 5 of the NATO Treaty[564]. Also, the European Council of the EU approved a document in which the Fifteen (both members and non-members of NATO) expressed their adhesion to the US thesis[565].

---

[562] UNGA, Resolution 56/1 "Condemnation of terrorist attacks in the United States of America", 12 September 2001.

[563] GRAY, C., *International Law…, op. cit.,* p. 200.

[564] Statement by the North Atlantic Council, NATO Press Releases (2001) 124, 12 September 2001, available at https://www.nato.int/docu/pr/2001/p01-124e.htm, [visited on 1 July 2018]; see also KOUZMANOV, K., *NATO's response to the 11 September 2001 terrorism: lessons learned*, Thesis, Naval Postgraduate School, Monterrey , 2003, p. 15.

[565] COUNCIL OF THE EU, *Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001*, Doc. SN 140/01, available at https://www.consilium.europa.eu/media/20972/140en.pdf, [visited on 2 July 2018], where it stated that "on the basis of Security Council Resolution 1368, a riposte by the US is legitimate […] The Member States of the Union, each according to their means, are willing to commit

It should be noted that before the UNSC adopted Resolutions 1368 and 1373 of 2001, the NATO provided that "Any armed attack on the territory of the allies, from whatever direction, would be covered by articles 5 and 6 of the Washington Treaty"[566], where it includes acts of terrorism since they are assumed as threat to the security of NATO members.

In fact, after the events of 11 September, some scholars have alleged that the prohibition of the use of force that has already been limited to inter-State relations, has been extended to private groups as "terrorism", and that States can invoke the right of self-defence[567]. Most of the legal experts and commentators support the right of self-defence against an armed attack by non-State actors without substantial involvement of a State[568]. In this sense, Kretzmer mentions that "The view that an attack by non-State actors that is not imputable to a State cannot constitute an 'armed attack' has been rejected by the vast majority of publicists" [569]. Moreover, Gray remarks that,

> "a wide view of the precedential significance of *Operation Enduring Freedom* might be asserted whereby States are now free to act in self-defence against

---

to such actions [...] Actions that can be directed against the States that help, support or shelter terrorists [...] ", p. 1.

[566] NATO, *The Final Declaration of the Washington Summit*, of 23- 25 April 1999, article 24, available at https://www.nato.int/cps/en/natohq/official_texts_27433.htm, [visited on 24 April 2018] .

[567] FRANCK, Th. M., "Terrorism...", *op. cit*., p. 840; MURPHY, S. D., "Terrorism and the concept of 'armed attack' in article 51 of the UN Charter", *HILJ,* 43, 2002, p. 42-51, at p. 50*;* TAMS, C. J., "Swimming with the tide or seeking to stem it? Recent ICJ ruling on the law on self-defense*", RQDI,* 18, 2005, p. 275-90; SCHRIJVER, N. J.*,* "The future of the Charter of the United Nations", *UNYB,* 10, 2006, p. 1-34, at p. 21-22; and RAO, P. S., "Non-State actors and self-defence: a relook at the UN Charter article 51", *Indian Journal of International Law*, 56(2), 2016, p. 127-171, at p. 141.

[568] See DINSTEIN, Y., *War, Aggression..., op. cit.,* p. 245-246; LUBELL, N., *Extraterritorial*..., *op. cit*., p. 35; CASSESE, A., *International law*, *op. cit*., p. 355; GREENWOOD, Ch., "International Law and the pre-emptive use of force: Afghanistan, Al-Qaida, and Iraq", *San Diego International Law Journal,* 4, 2003, p. 7-37, p. 7; FRANCK, Th. M., "Terrorism...", *op. cit*, p. 839; PAUST, J., "Use of armed force against terrorists in Afghanistan, Iraq and beyond", *Cornell International Law Journal,* 35, 2002, p. 533-557, at p. 533; STAHN, C., "Terrorist acts as 'armed attack': the right to self-defense, article 51(1/2) of the UN Charter, and international terrorism", *Fletcher Forum World Affairs*, 27, 2003, p. 35-54, at p. 35; SCHMITT, M. N., *Counter –terrorism and the use of force in International Law*, The George C. Marshall European Center for Security Studies, The Marshal Center Papers, No. 5, 2002, p. 25; MURPHY, S. D., "Self-Defense and...", *op. cit*., p. 62; and GILL, T. D., *et al*., (eds.), *Yearbook of International Humanitarian Law*, Springer, 17, 2014, p. 341.

[569] KRETZMER, D., "The inherent right to self-defence and proportionality in *jus ad bellum*", *EJIL,* 24(1), 2013, p. 235-282, at p. 246.

> the threat of any sort of terrorist attack on their nationals or their territory, even in the absence of any Security Council resolution, and even where the State against whose territory the action is taken had no involvement in any sort of support for the terrorists"[570].

Also, they claim that the right of self-defence is an inherent right which does not depend upon any prior breach of International Law by a State[571]. According to Dinstein, an act of violence by an armed band or terrorist group which is not imputed to another State but had originated in another State can amount to an armed attack under the meaning of the right of self-defence. Then, he refers to an "act of armed aggression" by mercenaries against the State in the UNSC Resolutions 405 and 419 in 1977[572] while the UNSC did not suggest that in order to constitute an armed attack another State must be involved[573].

Nevertheless, there is not unanimity and there have recently been serious controversies about the doctrine. The UN High-level Panel in its Report to the Secretary-General in 2004 which was adopted in 2005 by the UNGA Resolution *World Summit outcome,* affirmed that relevant provisions of the UN Charter are sufficient to address full range of all threats to international peace and security without deal with the questions particularly, when the right of self-defence is lawful[574].

Then, under the coverage of the UNSC Resolutions 1368 and 1373, the US, in collaboration with the UK, began military operations in Afghanistan to overthrow the Taliban regime[575]. Has there really been an extension of the right of self-defence?

---

[570] GRAY, Ch., *International Law…, op. cit.,* p. 202.

[571] *The Chatham House principles*…, *op. cit*., p. 970.

[572] UNSC, Resolutions 405, 14 April 1977 and Resolution 419, 24 November 1977.

[573] DINSTEIN, Y., *War, aggression…, op. cit.,* 2011, p. 245.

[574] UNGA, Resolution A/RES/60/1, "World Summit Outcome", 16 September 2005, par. 79; see also ROSTOW, N., "International Law and the use of force: a plea for realism", *YJIL*, 34(2), 2009, p. 549-557, at p. 553-554.

[575] For example, see the letters dated on 7 October 2001 that both the US and the UK governments they submitted to the UNSC, Doc. S/2001/946 and 947.

The UNSC Resolution 1368 invoked the right of self-defence without referring to the approval of military measures within the framework of the Chapter VII. This approval was not necessary if the use of force was carried out in the exercise of the right of self-defence. Likewise, the alleged extension of figure of the right of self-defence carried out by the UNSC has more relation with the right of self-defence "in accordance with the Charter of the United Nations" (literally affirmed in the two resolutions) than with the customary law on the self-defence that the ICJ recognized in the *Nicaragua case*. The problem is that in this case there was a doubt that there had been an "armed attack" within the meaning of article 51 of the UN Charter, since there was no intervention of the armed force of any State. Also, it is doubtful that in this case the armed response would meet the requirements of immediacy, provisionality and subsidiarity.

Moreover, it does not seem that this unique precedent is sufficient to change a norm so consolidated, especially when the position of three of five permanent members of the UNSC disagreed with armed action of the US and the UK against Iraq based on *preventive* strategic conceptions.

In fact, the operations of the UNSC in the Gulf and Afghanistan conflicts, deviated from the conventional prescriptions of article 51, have led to the legal question of whether a process of *desuetude* of the prescribed in the Charter has begun[576]. The legality of the US action could be based on the fact that the armed attack may consist on an indirect aggression by armed bands that are supported by a State (Afghanistan).

As seen above, the references to the right of self-defence contained in the UNSC resolutions and the approval of the armed reaction by several international organizations (UN, NATO, or EU) and the majority of the international community would be equivalent to accepting this extension of the right of self-defence recognized in the Charter.

However, the doctrine wonders whether the gravity of the attacks caused by the new form of global terrorism would have generated a new customary *lex specialis* that would broaden

[576] DEL VALLE, A., "¿Legítima defensa? Primer balance para el Derecho Internacional tras los atentados del 11 de septiembre de 2001", *Tiempo de Paz*, 64, 2002, p. 6-17, at p. 16-17.

the notion of armed attack to grave massive terrorist actions that States could respond with the exercise of a new modality of the right of self-defence. This new customary rule would be deduced from the acceptance by the international community of the US military response against Afghanistan[577].

If this is the case, it would be necessary to establish limits and conditions in which the States could resort to force in these situations; otherwise, the door would remain open to possible actions unilaterally decided by the most powerful States under the pretext of fighting against terrorism. It seems clear that, in these exceptional cases, apart from meeting the traditional requirements demanded by self-defence, it would also be necessary to have the UNSC's approval[578].

In any case, it is difficult to maintain that there has been the birth of a new customary norm since, on the one hand, the consensus manifested by the international community in 2001 to accept the right of self-defence of the US only existed as long as the commotion for events lasted and, on the other hand, the reaction of the international community has not been the same in relation to other attacks of similar characteristics (London, Bali, Paris or Barcelona).

In this context, Corten asserts that the declaration of the right of self-defence in the UNSC Resolutions 1368 and 1973 after 11 September events has never challenged or changed the existing law since it has been recognized by the UN Charter. In fact, paragraph 3 of the UNSC Resolution 1368 by saying that "calls on all States to work together urgently to bring to justice the perpetrators, organizers and sponsors of these terrorist attacks […]", it

---

[577] CONDORELLI, L., "Les attentats du 11 Septembre et leurs suites: où va le Droit International?", *RGDIP*, 105 (4), 2001, p. 829-848, at p. 843; and BERMEJO, R., "El Derecho Internacional frente al terrorismo: ¿nuevas perspectivas tras los atentados del 11 de septiembre?" *AEDI*, 17, 2001, p. 5-24, at p. 21. About the armed action in Afganistan in 2001 and 2002, see, among others, SCHRIJVER, N., "Responding to international terrorism: moving the frontiers of International Law for 'Enduring Freedoms'", *NILR*, 48(3), 2001, p. 271-291, at p. 271; GONZALEZ, J. A., "Los atentados del 11 de septiembre, la operación <libertad duradera> y el derecho de legítima defensa", *REDI*, 63, 2001, p. 248; GUTIÉRREZ, C., "¿No cesaréis de citarnos leyes viendo que ceñimos espadas?", *AEDI*, 2001, p. 25-38, at p. 25; and SAURA, J., "Some remarks on the use of force against terrorism in contemporary International Law and the role of Security Council", *Loyola of Los Angeles International & Comparative Law Review*, 26 (7), 2003, p. 7-30, at p. 23.

[578] CASANOVAS, O., "El principio…", *op. cit.*, p. 1077.

indicates that in the case-scenario that a State is responsible for supporting terrorist acts, it can be characterized as an armed attack[579].

Furthermore, Gray affirms that the UNSC Resolutions 1368 and 1373 indicate that its members were willing to accept legality of right of self-defence against terrorist attacks. Although, both resolutions referred to the right of self-defence in its preamble rather than in the operative part of resolutions, it was transparent that members were willing to accept the right of self-defence by the US against terrorist attacks[580]. Finally, Tams asserts that in the event to accept the right of self-defence against all type of armed attack by terrorist group independent of any State involvement, it is not clear what will remain from the rule of attribution in International Law based on the ICJ's view on the definition of aggression to constitute an armed attack[581].

It seems that the right of self-defence is not an adequate response to fight against international terrorism, even though it has been invoked regularly. In practice, many armed actions carried out by the States invocating the right of self-defence rather constitute an *armed retaliation* that is prohibited by International Law or even *aggressions.*

The evolution of customary and conventional aspects of the principle of self-defence can merge in practice of States. The evolution of self-defence is clear through recent State practice which has been constant and general[582]. Since the events of 11 September 2001, the wide support of self-defence against armed attack by non-State actors without substantial State involvement has been evidenced in recent State practice[583].

---

[579] CORTEN, O., *The law against war…, op, cit.,* p. 181-182; see also SHAH, S. A. "War on terrorism: self defense, operation enduring freedom, and the legality of US drone attacks in Pakistan", *Washington University Global Studies Law Review,* 9(1), 2010, p. 77-129, at p. 93.

[580] GRAY, C., *International law …, op. cit.,* p. 202.

[581] TAMS, C. J., "The Use of Force...", *op. cit*., p. 184.

[582] VAN STEENBERGHE, R., "Self-defence in response to attacks by non-State actors in the light of recent state practice: a step forward?", *LJIL,* 23(1), 2010, p.183-208, at p. 185-186.

[583] REINOLD, T., "State weakness...", *op. cit*., p. 244; O'CONNELL, M. E., "Dangerous departure", *AJIL,* 107, 2013, p. 380; and WILMHURST, E.; WOOD, M, "Self-Defence against non-State actors: reflections on the 'Bethlehem Principles'", *AJIL*, 107, 2013, p. 390-395, at p. 390; TRAPP, K. N., "The Turkish intervention against the PKK in northern Iraq-2007-08", in RUYS, T., *et al*. (eds.), *The use of force in International Law. A case-based approach*,

In this sense, in response to terrorist attacks to US embassies in Nairobi and Dar Es Salaam on 7th August 1998, the US invoked the right of self-defence against an armed attack to prevent repetition without asserting that the attacks were attributed substantially to a specific State[584]. The US alleged that they have *convincing evidence* that Bin Laden was behind these bombings and they have plans for more operations against the US interest[585]. Hence, the US launched missiles to sites in Afghanistan and Sudan that were under control of Bin Laden to produce chemical weapons and training terrorists[586]. However, international reaction to US operation was of virtual silence[587].

Also, in July 2006, Israel used the right of self-defence against Hezbollah into Lebanon to end firing of rockets by this group. These Israeli military operations were reported to the UNSC in the right of self-defence with a cautious approach to attribute responsibility to Lebanon[588]. Likewise, between 2008 and 2014 Israel launched three major operations against Gaza[589]. In this regard, *Operation Cast Lead* during December 2008 until January 2009, Israel launched a military reaction against Hamas group into Palestinian territory to destroy its capacity to fire rockets and missiles to Israel, and this its military operation is

---

OUP, 2018, p. 689-701, at p. 700; and TOMAS, C.; BRUCKNER, W., "The Israeli intervention in Lebanon-2006", in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 673-688, at p. 282 and 287.

584 UN, Doc S/1998/780, of 20 August 1998.

585 LOBEL, J., "The use of force...", *op. cit*., p. 537.

586 RISEN, J., "Question of evidence: a special report. To bomb Sudan Plant, or not: a year later, debates rankle", *New York Times*, 27 October 1999, available at https://www.nytimes.com/1999/10/27/world/question-evidence-special-report-bomb-sudan-plant-not-year-later-debates-rankle.html, [visited on 29 June 2018].

587 LOBEL, J., "The use of force...", *op. cit*., p. 556-557; see also "Sudan demands U.S. apology for missile attack", *CNN*, 23 August 1998, available at http://edition.cnn.com/WORLD/africa/9808/23/sudan.apology/,]visited on 1 April 2018[.

588 Israel declared that "Responsibility for this belligerent act of war lies with the government of Lebanon from whose territory these acts have been launched into Israel. Responsibility also lies with the governments of Iran and Syria, which embrace and support those who carried out this attack"; Letter from the Permanent Representative of Israel, UN Doc. S/2006/515, of 12 July 2006; see also GRAY, C., *International law and ..., op. cit*., p. 215.

589 See HENDERSON, Ch., "Israel military operations against GAZA: operation Cast Lead (2008-2009), operation Pillar of Defence (2012), and Operation protective Edge (2014)", in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 729-748, at p. 729.

reported to the UNSC under the right of self-defence[590]. Israel justification of the use of force under the right of self-defence against Hezbollah and Hamas has been recognized by many States expressly[591]. However, some States condemned Israel mainly because of its unnecessary or disproportionate force unleashed by Israel in response to the attacks that were committed by the non-State actors[592].

In addition, Ethiopia justified its military intervention in 2006 against *Union Islamic Court* (UIC) in territory of Somalia by recourse to the right of self-defence, asserting that such terrorist groups had declared Jihad on Ethiopia. The military action taken by the Transitional Federal Government of Somalia and Ethiopia was a "legitimate exercise of the inherent right of self-defence consistent with the United Nations Charter"[593]. Also, Prime Minister of Ethiopia Meles Zenawi in the Press Conference on 26 June 2007 asserted that

[590] UN, Doc. S/2008/814, of 24 December 2008; and UN, Doc. S/2008/816, of 27 December 2008.

[591] See, for instance, in regard to the Israeli intervention in Lebanon: statements from Argentina, UN Doc. S/PV.5489, at 9; Japan, UN Doc. S/PV.5489, at 12; United Kingdom, UN Doc. S/PV.5489, at 12; Peru, UN Doc. S/PV.5489, at 14 and UN Doc. S/PV.5493 (Resumption 1), at 4; Denmark, UN Doc. S/PV.5489, at 15; Slovakia, UN Doc. S/PV.5489, at 16, and UN Doc. S/PV.5493, at 19; Greece, UN Doc. S/PV.5489, at 17, and UN Doc. S/PV.5493 (Resumption 1), at 3; US, UN Doc. S/PV.5493, at 17; Russia (UN Doc. S/PV.5493 (Resumption1), at 2; Ghana, UN Doc. S/PV.5493 (Resumption 1), at 8; France (UN Doc. S/PV.5493 (Resumption 1), at 12; Finland which speaking on behalf of the European Union, UN Doc. S/PV.5493 (Resumption 1), at 16; Switzerland, UN Doc. S/PV.5493 (Resumption 1), at 18; Brazil, UN Doc. S/PV.5493 (Resumption 1), at 19; Norway, UN Doc. S/PV.5493 (Resumption 1), at 23; Australia, UN Doc. S/PV.5493 (Resumption 1), at 27; Turkey, UN Doc. S/PV.5493 (Resumption 1), at 28; Djibouti, UN Doc. S/PV.5493 (Resumption 1), at 32; Canada (UN Doc. S/PV.5493 (Resumption 1), at 39; and Guatemala, UN Doc. S/PV.5493 (Resumption 1), at 41. In regard to the Israeli intervention in Gaza, see for instance South Africa, UN Doc. S/PV.6060, at 8; Italy, UN Doc. S/PV.6060, at 13; Vietnam, UN Doc. S/PV.6060, at 13; Costa Rica, UN Doc. S/PV.6060, at 16; Belgium, UN Doc. S/PV.6060, at 17;Croatia, UN Doc. S/PV.6060,at 17.

[592] See, for instance the Israeli intervention in Lebanon, Russia, UN Doc. S/PV.5489, at 7; Argentina, UN Doc. S/PV.5489, at 9; Qatar, UN Doc. S/PV.5489, at 10; China, UN Doc. S/PV.5489, at 11; Japan, UN Doc. S/PV.5489, at 12; Congo, UN Doc. S/PV.5489, at 13; Tanzania, UN Doc. S/PV.5489, at 13; Denmark, UN Doc. S/PV.5489, at 15; Greece, UN Doc. S/PV.5489, at 17; France, UN Doc. S/PV.5489, at 17; Ghana, UN Doc. S/PV.5493 (Resumption 1), at 8; Brazil, UN Doc. S/PV.5493 (Resumption 1), at 19; New Zealand, UN Doc. S/PV.5493 (Resumption 1), at 33. See, e.g., regarding the Israeli intervention in Gaza, France, UN Doc. S/PV.6060, at 9; South Africa, UN Doc. S/PV.6060, at 9; Indonesia, UN Doc. S/PV.6060, at 10; Vietnam, UN Doc. S/PV.6060, at 13; Burkina Faso, UN Doc. S/PV.6060, at 15); Costa Rica, UN Doc. S/PV.6060, at 16; Belgium, UN Doc. S/PV.6060, at 17; Egypt, UN Doc. S/PV.6060, at 18; Turkey, UN Doc. S/PV.6061, at 10; Austria, UN Doc. S/PV.6061, at 14; Mexico, UN Doc. S/PV.6061, at 19; Argentina, UN Doc. S/PV.6061 (Resumption 1), at 8; Pakistan, UN Doc. S/PV.6061 (Resumption 1), at 10; Iceland, UN Doc. S/PV.6061 (Resumption 1), at 15; Ecuador, UN Doc. S/PV.6061 (Resumption 1), at 16.

[593] UNSC, Doc. S/2007/436, of 18 July 2007, par. 29.

they were "taken self-defensive measures and started counter-attacking the aggressive extremist forces of the Islamic Courts and foreign terrorist groups"[594].

Moreover, Turkey started a series of military operations against PKK into territory of Iraq in February 2008. The Turkey incursion had not been reported to the UNSC in justification of the right of self-defence, but several reasons showed that Turkey's reaction was under article 51 of UN Charter[595]. Although many States did not expressly approve the Turkish operation, they did not condemn it and they merely recommended Turkey to resort to proportionate force in the fight against PKK in Iraq[596]. Other States did not oppose (ignore) Turkish operations in the right of self-defence in front of the PKK[597].

More recently, an International Coalition of more than sixty States have invoked the right of self-defence against the *Daesh* (derived from Arabic) or *ISIL* (UN official documents); a terrorist group that proclaimed itself as a "world caliphate" on 29 June 2014[598]. Then, to confront Daesh threats, the UNSC Resolution 2249 declared,

---

[594] *The Guardian*, of 9 July 2007; see also, ALLO, A. K., "Ethiopia's armed intervention in Somalia: The legality of self-defense in response to the threat of terrorism", *Denver Journal of International Law and Policy*, 39, 2010, p. 139.

[595] Among others, the Turkish Prime Minister Recep Erdogan in October 2007 explicitly stated that "We have reached the point of self-defence, and we are ready to do whatever is necessary in light of common sense" in order to adoption by the Turkish Parliament of a plan for incursion to PKK in North of Iraq"; see *New York Times*, of 17 October 2007; and also Turkey did not assert any other justification to use of force as authorization of the UNSC, humanitarian intervention or consent of territorial State (Iraq); see VAN STEENBERGHE, R., "Self-defence…", p. 188.

[596] TYSON, A. S.; WRIGHT, R., "U.S. helps Turkey hit rebel Kurds in Iraq", The *Washington Post*, 18 December 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/12/17/AR2007121702150.html??noredirect=on,]visited on 6 September 2017[; see also the EU that addressed Turkey to rely on the *ius ad bellum* concept of proportionality to carrying out military operations and limit its military activities to those which are absolutely necessary to the protection of the Turkish population from terrorism, "EU Presidency statement on the military actions undertaken by Turkey on Iraqi territory", 25 February 2008, available at http://www.eu2008.si/en/News_and_Documents/CFSP_Statements/February/0225MZZturkey.html, [visited on 4 August 2017].

[597] VAN STEENBERGHE, R., "Self-defence…", *op. cit.*, p. 194; TRAPP, K. N., "The Turkish intervention against the PKK...", *op. cit.*, p. 694.

[598] CORTEN, O., "The military operations against the 'Islamic State' (ISIL or Daesh)-2014" in RUYS, T., *et al.*, *The use of force in International Law. A case-based approach*, OUP, 2018, p. 873-898, at p. 873.

> "Calls upon Member States that have the capacity to do so to take all necessary measures, in compliance with international law [...], on the territory under the control of ISIL also known as Da'esh, in Syria and Iraq, to redouble and coordinate their efforts to prevent and suppress terrorist acts committed specifically by ISIL [...]"[599].

While it is true that this Resolution does not invoke Chapter VII of the Charter, it seems that it gives legal support to the actions of the International Coalition against the *Daesh*[600].

Moreover, after the events of Paris on 13 November 2015, which resulted in dozens of victims, France asserted that it is victim of an 'armed aggression' to justify the right of self-defence[601]. In this sense, members of the EU agreed for first time to activate article 42(7) of the treaty on European Union after the events in Paris[602]. According to this article

> "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States"[603].

It is also noticeable the silence of the international community before Turkey's new incursion against Kurdish militia People's Protection Units (YPG) in Afrin (Syria) in 2018,

---

[599] UNSC, Resolution 2249 on threats to international peace and security caused by terrorist acts, 20 November 2015, par. 5.

[600] CERVELL, M. J., *La Legítima defensa..., op. cit.*, p. 237-244; in particular p. 240; see also PETERS, A., "German Parliament decides to send troops to combat ISIS, based on collective self-defence in conjunction with SC 2249", *EJIL Talk*, December 2015, available at http://www.ejiltalk.org,]visited on 21 June 2018[; BERDUD, CARLOS ESPALIÚ, "The EU response to the Paris terrorist attacks and the reshaping of the rights to self-defence in International Law", *Spanish Yearbook of International Law,* 20, 2016, p. 183-207, at p. 199-200; and MURRAY, C. R. J.; O'DONOGHUE, A., "Towards unilateralism? House of Common oversight of the use of force", *ICLQ*, 65(2), 2016, p. 305-341, at p. 26.

[601] UNSC, Doc S/PV.7565 on "Threats to international peace and security caused by terrorist acts", 20 November 2015, p. 2.

[602] COUNCIL OF EU, Outcome of the Council Meeting, 3426th Council Meeting, Foreign Affairs, 16 and 17 November 2015, 14120/15, p. 6.

[603] Consolidated version of the Treaty on European Union, 7 February 1992.

after army Kurdish fighters opened fire on Turkish troops in border[604]. In this regard, Turkey claimed that "the operation is being carried out within the right of self-defence and with respect to Syrian territorial integrity"[605]. However, the lack of necessity and proportionality is evident in Turkish continued military operations.

Thus, although it is not absolutely clear that exists a real approval to the right of self-defence against armed attack by non-State actors without a State substantially involved in the attack, at least as we have seen how the recent State practice shows that the international community now has a tendency towards the authorization of the right of self-defence against an armed attack by non-State actors[606].

This new tendency to accept the right of self-defence against non-State actors has also been confirmed by different international legal bodies. In this sense, it is valuable to refer to the *Chatham House Principles* of 2005*,* already mentioned; to the IDI Resolution in 2007 declared that "In the event of an armed attack against a State by non-State actors, article 51 of the Charter as supplemented by customary International Law applies as a matter of principle"[607], and subsequently it affirms that "If an armed attack by non-State actors is launched from an area beyond the jurisdiction of any State, the target State may exercise its right of self-defence in that area against those non-State actors"[608]. Then, it clearly

---

[604] "Turkey targets Kurdish positions in Syria's Afrin", *The New Arab*, of 20 January 20018.

[605] "Turkish jets hammer Syrian town to oust US-backed Kurdish militia", *CNN News*, 21 January 2018, available at https://edition.cnn.com/2018/01/20/middleeast/turkey-syria-military-operation/index.html [last visited 20 June 2018].

[606] See RUYS, T., "*Quo vadit jus ad bellum*?: a legal analysis of Turkey's military operation against the PKK in Northern Iraq", *Melbourne Journal of International Law*, 9(2), 2008, p. 334-363, at p. 350-358; BETHLEHEM, D., "Self-defence against...", *op. cit*., p. 769-777; CASSESE, A., "Article 51", in COT, J. P.; *et al*. (eds.), *La Charter des Nations Unies,...,op. cit*., p. 1329-1360; FRANCK, Th. M., "Terrorism ...", *op. cit*., p. 840; KRETZMER, D., "The inherent right to self-defense...", *op. cit*., p. 246-250; MURPHY, S. D., "Self-defence and...", *op. cit*., p. 62-76; WEDGWOOD, R., "The ICJ Advisory Opinion on the Israeli...", *op. cit*., p. 52-62; TRAPP, K. N., "Back to basics...", *op. cit*., p. 141-156; TAMS, C. J., "The Use of Force...", *op. cit*., p. 359-395; RATNER, S. R., "Self-defense against terrorists: the meaning of armed attack", *MJIL*, 2012, p. 1-20, at p. 2; NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit*., p. 1418; DE SOUZA, I. M. L., "Revisiting the right of self-defence against non-State armed entities", *CYIL*, 53, 2015, p. 202-243, at p. 202; PETERS, A., "German Parliament decides to send troops...", *op. cit*.; or CERVELL, M. J., *La legítima defensa..., op. cit.*, p. 225-226.

[607] IDI, 10A Resolution "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., article 10.

[608] *Ibid*, article 10(ii).

establishes that article 51 is applicable in the case of an armed attack of a non-State actor from outside the jurisdiction of any State.

Moreover, the IIFFMCG in its *Report on the conflict in Georgia* in 2009, applied article 51 of the UN Charter to the use of force, utilized among Georgia, Abkhazia and South Ossetia[609]. Lately, ILA, *Draft Report on aggression and the use of force* of 2016, asserts that "Article 51 does not specify that the armed attack which gives right to self-defence must have been carried out by a State, and therefore leaves rooms for textual reading that includes attacks by non-State actors", and adds that States are able to defend themselves against attacks from outside their border, which is more highlighted through State practice since 2001[610]. Thus, according to ILA "if the armed attack is only attributable to the non-State actor, the victim State may have a right to self-defence against the armed group but not against the State"[611].

In addition, *Tallinn Manual 2.0,* after considering that international community characterized the 11 September attacks as an armed attack triggering the inherent right of self-defence, affirms that "such State practice appears to signal a willingness of States to apply the right of self-defence to attacks conducted by non-State actors"[612].

Therefore, despite some doctrine has doubts about the legal applicability of the right of self-defence against non-State actors[613], according to the States practice and the approval of the majority of the individual and collective doctrine to use of such right to cope with new threats of non-State actors, we can accept the exercise of the right of self-defence

[609] IIFFMCG, *Report on the conflict in Georgia*, *op. cit.,* vol. I, p. 25; and vol. II, p. 127 and 134; see HENDERSON, Ch.; GREEN, J. A., "The *ius ad bellum* and entities short of statehood in the Report on the conflict in Georgia", *ICLQ,* 59(1), 2010, p. 129-139.

[610] ILA, *Draft Report on aggression and the use of force, op. cit*., 2016, p. 11.

[611] *Ibid*, p. 12.

[612] *Tallinn Manual 2.0*, *op. cit*., rule 18, par. 18.

[613] CHARNEY, J. I., "The use of force against terrorism and International Law", *AJIL*, 95(4), 2001, p. 834-841, at p. 835-839; BYERS, M., "Terrorism, the use of force and International Law after 11 September", *ICLQ,* 51(2), 2002, p. 401-414, at p. 411; ANTONOPOULOS, C., "Force by armed groups as armed attack and the broadening of self-defence", *NILR,* 55(2), 2008, p. 159-180, at p. 162-172; or ENABULELE, A. O., "Use of force by international/regional non-State actors: no armed attack, no self-defence", *European Journal of Law Reform*, 12, 2010, p. 209-229, at p. 216.

against an armed attack by non-State actors even without a State substantially involved in such attack, at least against those groups involved in terrorist activities[614].

4. *The accumulation of events theory*

As it has been seen *supra,* armed acts must have sufficient gravity to be qualified as armed attacks in sense of article 51 of the UN Charter. However, according to the *accumulation of event theory*

> "a State that suffers minor armed attacks during a period of time could exercise the right of self-defence by taking into account the whole series of attacks against it. It is also argued that different attacks would be considered as part of the same conflict, and that continuous are the situations where an armed conflict having come to an end, another attack has taken place and so forth"[615].

Recently, there are important controversies about whether a series of acts can amount to degree of gravity to constitute an armed attack to justify the right of self-defence. The ICJ in *Nicaragua case* mentioned that when there is lack of evidence it is difficult to determine whether the invasion to the territory of Honduras and Costa Rica individually or collectively can amount to an armed attack[616]. This line is followed in the *Oil platforms* case where it is declared that "even taken cumulatively […] these incidents do not seem to the Court to constitute an armed attack"[617]. Hence, it seems the ICJ "leave open the possibility of an accumulation of events"[618] and "did not exclude the possibility of a cumulative effect armed attacks otherwise minor"[619].

---

[614] In fact, the UNSC in its Resolutions 1368, 1373 and 2249 only refers to the right o self defence in response to terrorist attacks.

[615] IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., p. 114.

[616] ICJ, *Nicaragua case, op. cit.,* par. 231.

[617] ICJ, *Oil platform case, op. cit*., par. 64.

[618] GRAY, Ch, *International law …, op. cite,* p. 164.

[619] IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*.,, p. 114.

Moreover, the Court in the *Land and Maritime Boundary case* did not mention conceptual basis and constrained its view to the non-attribution of the facts to one of the parties[620]. Furthermore, in the *Armed activities in the territory of the Congo* case declared that "even if this series of deplorable attacks could be regarded as cumulative in character, they still remained non-attributable to the DRC"[621]. It looks that the Court implicitly accepted that numbers of attacks by Allied Democratic Force can be an armed attack based on theory of accumulation of smaller attacks to constitute an armed attack.

Thus, in order to clarify this issue, the ICJ avoided any ruling on this theory. However, the Court implicitly supported that series of acts that are below the level of an armed attack can cumulatively amount to an armed attack in sense of article 51[622]. In this sense, Gray claims that "the Court apparently contemplated the possibility of an 'accumulation of events' model of armed attack, but did not discuss this controversial question"[623].

It is noticeable that in the *Nicaragua case,* some judges such as Singh[624] and Jennings[625] implicitly accepted this view. In contrast, some judges, such as Simma rejected this approach in the *Oil Platform case*, where it was declared that "there is in the International Law on the use of force no 'qualitative jump' from iterative activities remaining below the threshold of article 51 of the Charter to the type of 'armed attack' envisaged here"[626]. According to Green, "there has been general acceptance of the accumulation of events theory by the Court, and this can be seen to pose further problems in attempting to determine the lawfulness of any given action ostensible taken in self-defence"[627].

---

620 ICJ, *Case concerning land and maritime boundary between Cameroon and Nigeria* (Cameroon *v.* Nigeria: Equatorial Guinea intervening), judgment of 10 October 2002, *ICJ Reports* 2002, par. 323.

621 ICJ, *Armed activities in territory of Congo case , op. cit*., par. 146.

622 DINSTEIN, Y., *War, aggression…, op. cit.*, p. 211; and O'CONNELL, M. E., *The power and purpose of International Law*, OUP, 2008, p. 182.

623 GRAY, Ch, *International Law..., op. cit*., p. 165.

624 ICJ, *Nicaragua case*, *op. cit*., separate opinion of judge Nagendra Singh, par. 154.

625 *Ibid*, separate opinion of judge Jennings, par. 543.

626 ICJ, *Oil Platforms case*, *op. cit*, par. 14.

627 GREEN, J. A., *The International Court ..., op. cit.,* p. 44.

This theory arises questions about necessity and proportionality criteria in the use of self-defence. Some scholars claim that "the notion of continuous armed conflict is a dangerous one open to abuse"[628]. However, part of the doctrine mentions that "General practice seems to be that the UNSC, in presence of separate periods of armed conflicts refuses to consider the latest as the continuation of a previous one"[629]. Thus, they believe that the accumulation of events theory has received cold shoulder by the UNSC[630]. Gray claims that the UNSC just has not gone so far and it only has condemned disproportionate responses (for instance, by South Africa, Portugal, Israel or US) which were not related to the right of self-defence[631].

In this context, ILA affirms that "a number of incidents which alone might not be armed attacks might be seen as together being an armed attack" and asserts that in order to take account proportionate force to reaction in the right of self-defence can be related to the series of attacks, not simply the last one[632].

In fact, one of the challenge of the accumulations of events theory is the uncertain response about how many *minor attacks* are required to constitute an armed attack[633] to avoid to open the door to some abuses; for instance, in recent State practice, particularly Israel invasion against Gaza during 2008-2009, accumulative theory has been expressed by Israel officers claiming that Israel has the right to use of the self-defence in response to many weeks, months and years of attacks which its citizen were subject to deliberate terrorist

---

628 GREENWOOD, Ch., "International Law and the US air operation against Libya", *West Virginia Law Review, 89,* 1987, p. 953-956; and IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., p. 114.

629, IDI*, ibid*, p. 114.

630 LEVENFELD, B., "Israel's Counter-Fedayeen tactics in Lebanon: self-defence and reprisal under modern international law", *Columbia Journal of Transnational Law,* 21, 1982, p. 1-48, at p. 5-9; see also TAMS, C. J., "The use of force...", p. 359.

631 GRAY, C., *International Law..., op. cit.,* p. 164.

632 ILA, *Draft Report on aggression and the use of force, op. cit*., 2016, p. 4

633 LAURSEN, A., "The Judgment by the International Court of Justice in the *Oil Platforms* Case", *NJIL,* 2004, p. 135-160, at p. 155; and GREEN, J. A., *The International Court ..., op. cit.,* p. 44.

attacks[634]; however the legal scholars explicitly asserted that the firing of rockets from Gaza was not serious enough to amount to an armed attack and trigger the right of self-defence[635].

Although the accumulation of events theory in international community has not gained general acceptance, the growing international terrorism attacks have left the States with serious challenges that caused the decrease of their previous rejection to such theory. In this regard, Tams believes that "States seem to have shown a new willingness to accept the 'accumulation of events' doctrine which previously had received little support"[636].

C. **Other requirements to exercise the right of self-defence**

In the precedent sections, in relation to the exercise of the right of self-defence, we have seen the requirements established in the article 51 of the UN Charter; subsequently, we will analyse other requirements prescribed by general International Law: necessity, proportionality and immediacy.

1. *Necessity*

Traditionally, necessity requirement has been recognized as conditions to exercise the right of self-defence against armed attack by State in inter-State conflict[637]; however, this requirement is not explicitly mentioned in article 51 of the UN Charter. In this context, necessity and proportionality have customary character that supplement the UN Charter provision. Do not confuse the necessity to act in the right of self-defence against an armed attack with the defence of a State, the realization of State rights or the provocation.

---

[634] Israel Permanent Representative; Israel Ambassador Gabriela Shalev, see UNSC, Doc S/PV. 6060 on "the situation in the Middle East, including the Palestinian question", 31 December 2008.

[635] See "Israel's Bombardment of Gaza is not self-defence–It's a war crime", *Sunday Times*, of 11 January 2009; this article have been signed by many legal scholars such as I. Brownlie, R. Falk, C. Chinkin, and M. C. Bassiouni .

[636] TAMS, C. J., "The use of force...", *op. cit.*, p. 388.

[637] See OHLIN, J. D.; MAY, L., *Necessity in International Law*, OUP, 2016, p. 16.

a) *Inter-State necessity*

Requirements of right of self-defence is inferred primary of the *Caroline formula* in 1937, when Webster upon a strict view on responsive force to the ship *Caroline*, described necessity criterion as "instant, overwhelming, leaving no choice of means, and no moment of deliberation"[638]. This expression implicitly indicates that clear and absolute necessity must exist in order to justify the right of self-defence[639].

According to the general International Law, certain requirements are frequently mentioned as essential conditions to admit the exercise of the right of self-defence while

> "Reference is made, in particular, to the requirements that the action to be excused must, in the case in question, be 'necessary', that it must be 'proportional' to the objective which it is supposed to achieve, and that it must take place 'immediately'. These are, actually, merely three aspects of the same principle which serves as a basis for the effect, attributed to the situation of self-defence"[640].

Necessity criteria in the right of self-defence field, implies that the use of force is the only means that the State can resort to, not having others at their disposal to stop the armed attack[641]. As IDI pointed out, the right of self-defence only occurs when there is no lawful alternative practicable to prevent, stop or reject an armed attack ("*the only viable alternative*") until the effective intervention of the UNSC[642]. The necessity condition in the right of self-defence will exist while the State is being attacked until the UNSC takes the necessary measures to maintain international peace and security.

---

[638] Noted by Mr Webster to Mr Fox on 24 April 1841 in DAMROSCH L. F., *et al., International Law: cases and Materials,* West Academic*,* 2001, p. 923.

[639] PAUST, J. J., "Self-defence targeting...", *op. cit.*, p. 243.

[640] ILC, "State responsibility", *op. cit*., vol. II, part 1, 1980, p. 69.

[641] LAURSEN, A., "The use of force and (the State of) necessity", *VJTL,* 37, 2004, p. 485-526, at p. 494.

[642] IDI, "Present problems of the use of armed force in International Law. Humanitarian action*", op. cit*., p. 273.

That is, the necessity requirement indicates that the use of force under the right of self-defence is applicable when States realize that the use of force is the only possible alternative (*ultima ratio*) to maintain its integrity[643], or according to ILC, "is the only way for the State to safeguard an essential interest against a grave and imminent peril"[644].

It is noticeable that necessity requirement does not oblige to a victim State to exhaust *all* non-forcible responses before recourse to self-defence, but just non-forcible alternatives that are likely to be effective; in other words, the necessity has to be understood in the sense, "not so much of being the only alternative, but of those measures being more *adequate* or *convenient* to repel the previous armed attack"[645]. A defender State in good faith and on basis of time and facts must assess whether he can avert the attack without resorting to force[646].

Also, the ICJ outlined that "there is a specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary International Law"[647]; and affirmed that "response to the attack is lawful depends on the observance of the criteria of the necessity and the proportionality of the measures taken in self defence"[648]. In the case of *Armed activities in the territory of the Congo,* the Court considered that the conditions to justify the right of

---

[643] ICJ, *Nicaragua case*, *op. cit*., par. 237; see also TAMS, C. J.; DEVANEY, J. G "Applying necessity and proportionality to anti-terrorist self-defence", *Israel Law Review,* 45(1), 2012, p. 91-106, at p. 96; OPPENHEIM, L., quoted in ENABULELE, A.; BAZUAYE, B., *Teachings on basic topics in Public International Law*, Ambik Press, 2014, p. 379, where in part (c) he mentioned that "there is no practicable alternative to action in self-defence, and in particular another State or other authority which has the legal powers to stop or prevent the infringement does not, or cannot, use them to that effect".

[644] ILC, "Responsibility of States...", *op. cit*, vol. II, part 2, 2001, article 25.

[645] CERVELL, M. J., "Sobre la doctrina <unwilling or unable State> (¿podría el fin justificar los medios?), *REDI*, 70(1), 2018, p. 77-100, at p. 96-97, see also ILC, "State responsibility", Documents of the thirty-second session, *Yearbook of ILC*, vol. II, part 1, 1980, p. 69, par. 119; *The Chatham House principles*...," *op. cit.,* p. 967; IIFFMCG, *Report on the conflict in Georgia*, vol. II, *op. cit*., p. 248; and *Tallinn Manual 2.0, op. cit.,* rule 72, par. 2.

[646] *The Chatham House principles*...," *op. cit.,* p. 967; see also FOLEY, B. J., "Avoiding a death dance: adding steps to the International Law on the use of force to improve the search for alternatives to force and prevent likely harms", *Brooklyn Journal of International Law*, 29(1), 2003, p. 129-173, at p. 143.

[647] ICJ, *Nicaragua case*, *op. cit*., par. 176; and *Legality of nuclear weapons*, *op. cit*., par. 41; see also IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., p. 99.

[648] ICJ, *Nicaragua case*, *op. cit*., par. 194; and *Oil platform* case, *op. cit*., par. 74; see also par. 77.

self-defence of Uganda did not meet, in particular, the necessity and proportionality[649]. However, in this context, it did not refer to the immediacy and other requirements set forth in article 51 and in general International Law.

The requirement of necessity will only be met: firstly, when the use of force is necessary to stop the attack; in a broader sense, necessity to defend itself exists when, if no action is taken, there is a risk of losing a State asset because of the incoming attack; this implies an immediate relation in the time between the act of self-defence and the attack; the most frequent form of presenting the necessity to act in self-defence is simply to affirm the existence of an armed attack. In other words, the necessity derives from the existence of actual armed attack on territory of State which attack must be with sufficient gravity to affect the integrity of such State, as described in article 3(a) of UNGA Resolution 3314 (XXIX). In this context, ILC mentioned that "The reason for stressing that action taken in self-defence must be *necessary* is that the State attacked (or threatened with imminent attack, if one admits preventive self-defence) must not, in the particular circumstances, have had any means of halting the attack other than recourse to armed force"[650].

And secondly, the self-defence must be for a defensive purpose and not for other purposes such as retaliatory, deterrent or punitive[651]; the action must always be with defensive purpose and never endanger international peace and security. Necessity criteria to use the right of self-defence is not only limited to avert the initial armed attack, but also to prevent the occurrence of imminent attacks by the attacker[652]; the use of the right of self-defence is

[649] ICJ, *Armed activities in territory of Congo*, *op. cit.*, par. 174.

[650] ILC, "State responsibility", *op. cit.*, vol. II, part 1, 1980, p. 69.

[651] *Ibid*, p. 69; see also NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit.*, p. 1425; CORTEN, O., *The law against war…, op. cit.*, p. 484; and CASSESE, A., *International law, op. cit.*, p. 355.

[652] IIFFMCG, *Report on the conflict in Georgia*, vol. I, September 2009, par. 21; see also O'CONNEL, M. E., "Lawful self-defense...", *op. cit.*, p. 903; and RUYS, T., *'Armed Attack'…, op. cit.,* p. 518-519.

not restricted to expel attacking foreign troops from their territory; they may, in principle, pursue them across the border in order to secure the end of the attack[653].

Likewise, a victim State must determine that attack *aimed specifically* objective and it did not attack mistakenly. In other words, there must be specific *intention* to harm the ship, air flight, etc. Hence, mine and missile cannot constitute an armed attack on third State during conflict between two other States[654]. This approach was explicitly expressed by the ICJ in the *Oil Platform*[655].

Consequently, according to general International Law, the necessity requirement is a fundamental precondition to authorize the exercise of the right of self-defence; in the absence of necessity, any use of force would be unlawful.

b) *Necessity against non-State actors*

As it is mentioned, contemporary International Law extended the right of self-defence directly against an armed attack by non-State actors. However, there remains the question of how International Law can adapt necessity criterion to the right of self-defence outside inter-State relations.

In order to exercise the right of self-defence against an armed attack by States, assess necessity criteria is comparable between forcible and non-forcible use of force, but discern necessity criteria in the right of self-defence against armed attack by non-State actor in territory of another State, is in comparison between unilateral actions by a victim State or unilateral actions by a host State[656].

---

[653] GARDAM, J., *Necessity, proportionality and the use of force by States*, 35, CUP, 2004, p. 164; NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit.*, p. 1426; and also see IIFFMCG, *Report on the conflict in Georgia*, vol. II, September 2009, p. 272.

[654] GRAY, C., *International Law…, op. cit.,* p. 162; and DINSTEIN, Y., *War, aggression…, op. cit.*, p. 250.

[655] ICJ, *Oil Platform* case, *op. cit.,* par. 64.

[656] TAMS, C. J.; DEVANEY, J, G., "Applying necessity and...", p. 98.

As a general rule, there is a primacy of the action by host State[657]. If an armed attack occurs by non-State actors, according to the necessity condition, prior to resorting to the right of self-defence, the victim State has to request to the host State to suppress non-State actors acts. Alternatively, the victim State might cooperate with host State to repress such groups or may acquire consent of the host State to activate extraterritorial measures against non-State actors[658].

Thus, to justify the right of self-defence against an armed attack by non-State actors, victim State reaction is not primacy to host State. This idea is implied in recent State practice, where Turkey, the US and Israel frequently justified acts of self-defence against terrorist groups in territory of other States by the allegation that the host State had taken no action or that its respective State is unwilling or unable to eliminate threats[659].

In this context, there are three scenarios: first, if the host State supports non-State actors, therefore enforcement action by the host State against such groups seems unlikely[660]. In this case, it is clear that the reaction of the victim State in the right of self-defence against an armed attack by non-State actors seems necessary. This approach was evidenced by international community that supported the military action against *Al-Qaeda* in Afghanistan after realizing about the relationship between *Taliban* regime and *Al-Qaeda* organization since 1990[661].

Second, when the host State just tolerate non-State actors; does not actively support them or at least there is no evidence of support, this case seems a little more complicated[662]. In the practice, as it has seen *supra*, there are evidences of reaction to international

---

[657] *Ibid.*

[658] *The Chatham House principles …*", *op. cit.*, principle (f), p. 969.

[659] TAMS, C. J.; DEVANEY, J, G., "Applying necessity…, *op. cit.*, p. 98.

[660] RUYS, T.; VERHOEVEN, S., "Attacks by private actors and the right of self-defence", *Journal of Conflict and Security Law,* 10(3), 2005, p. 289-320, at p. 316.

[661] PAUST, J. J., "Use of armed force...", *op. cit.*, p. 533-557.

[662] RUYS, T.; VERHOEVEN, S., "Attacks by private actors…, *op. cit.*, p. 317; see also SCHACHTER, O., "The Use of Force against Terrorists in Another Country", *Israel Yearbook on Human Rights*, 19, 1989, p. 209-231, at p. 225-231.

community of resort to the right of self-defence in some sporadic cases; for instance, Turkey against PKK in the territory of Iraq and recently in Syria. Moreover, Russia has tried to justify such right of military interference in the territory of Georgia against Chechen rebel group[663] or Iran in front of Mujahedin-e-Khalq Organization (MKO) into territory of Iraq[664], where they claimed that the right of self-defence is applicable against terrorist groups inside the territory of another State when host States tolerate such groups in their territories. This approach might have derived from the duty of States to not allow their territories to be used to infringe the right of other States, according to the ICJ jurisprudence and the UNGA Resolutions[665] or implicitly in modern international conventions which have explicitly forbidden to give shelter to terrorists or any action of support to any act of aggression[666].

Nevertheless, the recent State practice indicates that if host States tolerate or harbour terrorist groups activities in their territories and therefore the victim State were to use the force under the pretext of the right of self-defence against non-State actors, to our understanding, such use of force would not be according to International Law. In fact, the mere *tolerance* of non-State actors that develop terrorist activities cannot authorize the recourse to the right of self-defence by a victim State[667].

Third, when recent State practice indicates that the exercise of the right of self-defence is necessary if a host State is merely *unable* to suppress threats in its territory. For instance,

---

663 Letter from the Permanent representative of the Russia Federation to the Secretary-General of the United Nations, UN Doc S/2002/1012, 11 September 2002; it is not clear whether Georgia was unable or unwilling to eradicate terrorist in its territory, however Russia justified its military operation into territory of Georgia, because of territorial State was unable or unwilling to counteract the terrorist threat.

664 Iran invasion in territory of Iraq to pursuit of Kurdish armed bands by invoke to right of self-defence, avoided international criticism. There was lack of evidence to attribute conduct of the MKO to Iraq; see FRANCK, Th. M., *Recourse to force: threats and armed attacks*, CUP, 2002, p. 64.

665 The Court view is that each State has a duty "not to allow knowingly its territory to be used for acts contrary to the rights of other States", ICJ, *Corfu Channel case*, *op. cit*., par. 4; see also UNGA Resolution 2625 (XXV), *op. cit*., pars. 8 and 9 of the principle of the prohibition of the threat or use of force.

666 For instance, African Union Non-Aggression and Common Defence Pact, 1st January 2005, where according to article 1, c (xi), aggression means "the encouragement, support, harbouring or provision of any assistance for the commission of terrorist acts and other violent trans-national organized crimes against a member State".

667 CERVELL, M. J., "Sobre la doctrina <unwilling or unable State>...", *op. cit*., p. 88-89.

as it is mentioned *supra*, in 2006 many States supported the Israel military response on the right of self-defence against Hezbollah in territory of Lebanon while this State was not in position to suppress Hezbollah activities[668]. Also, in Syria since 2014 some States such as the US, UK, Canada, Australia and Turkey in their letter to UNSC justified their action in self-defence because Syria was *unable* and *unwilling* to prevent the threat and attack of *Daesh* which was emanating from its territory[669].

However, some time to distinguish between the last two scenarios, unwillingness and inability, is very difficult and their line is very close. In this context, some scholars claim that the "self-defence is an inherent right and is not dependent upon any prior breach of International Law" by the host State[670]; hence, unable and unwilling test can activate the necessity requirement of the right of self-defence[671]. In this regard, Deeks held that:

> "A victim State must consider not just whether the attack was of a type that would require it to use force in response to that non-State actor, but it also must evaluate the conditions in the State from which the non-State actor launched the attacks. This latter evaluation is where, absent consent, States currently employ the 'unwilling or unable' test to assess whether the territorial State is prepared to suppress the threat. If the territorial State is

---

[668] Among others, Canada, "Harper sides firmly with Israel", Canadian Press, 13 July 2006, available at https://web.archive.org/web/20080620182821/http://www.theglobeandmail.com/servlet/story/RTGAM.20060713.wHarper0713/BNStory/Front; USA, "President Bush and German Chancellor Merkel participate in press availability", 13 July 2006, available at https://georgewbush-whitehouse.archives.gov/news/releases/2006/07/20060713-4.html, [visited on 3 April 2018].

[669] US, UN, Doc. S/2014/695, of 23 September 2014; Canada, UN Doc. S/2015/221, of 31 March 2015; Turkey, UN, Doc. S/2015/563, of 24 July 2015; Australia, UN, Doc. S/2015/693, of 9 September 2015 and UK, Cameron *Statement in the House of Commons on His Response to the Foreign Affairs Select Committee (FAC) Report on Military Operations in Syria*, 26 November 2015, available at https://www.gov.uk/government/speeches/pm-statement-responding-to-fac-report-on-military-operations-in-syria, [visited on 23 March 2018].

[670] *The Chatham House principles..., op. cit*., p. 970; TOMAS, C.; BRUCKNER, W., "The Israeli intervention in Lebanon...", *op. cit*., p. 282; and DINSTEIN, Y., *War, aggression..., op. cit*., p. 245

[671] DINSTEIN, Y., *War, aggression…", op. cit*., p. 292-293; see also the *Chatham House Principles...,* p. 570-571; SCHRIJVER, N.; VAN DEN HERIK, L., *Leiden Policy Recommendations on counter-terrorism and International Law* 1 April 2010, published in *NILR,* 57(3), 2010, p. 531-550, at p. 543, par. 32; and ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 12, ILA affirms that "the unwilling or unable test should be viewed as a component of the necessity criteria".

> neither willing nor able, the victim State may appropriately consider its own use of force in the territorial State to be necessary and, if the force is proportional and timely, lawful"[672].

Thus, according to this view, when a State is *unable* and *unwilling* to control a non-State actor located in its territory, a victim State in last resort is justified to recourse to self-defence against this group into the territory of the State where it is located[673]. If a host State is clearly unable to overcome non-State actors, it must seek other States assistance. Otherwise, it would be accused of violating the rule that obliges a State to attempt to repel any armed attack emanating from its territory[674]. In this sense, the UNSC in Resolution 1368 (2001)

> "Calls on all States to work together urgently to bring to justice the perpetrators, organizers and sponsors of these terrorist attacks and stresses that those responsible for aiding, supporting or harbouring the perpetrators, organizers and sponsors of these acts will be held accountable".

Moreover, the UN Special Rapporteur Philip Alston asserts that targeted killings conducted by one State in the territory of a second State do not violate the second State's sovereignty. In this sense it asserts that if

> "State has a right under international law to use force in self-defence under Article 51 of the UN Charter, because (i) the second State is responsible for an armed attack against the first State, or (ii) the second State is unwilling or unable to stop armed attacks against the first State launched from its territory. International law permits the use of lethal force in self-defence in

---

672 DEEKS, A. S., "'Unwilling or unable': towards a normative framework for extraterritorial self-defence", *Virginia Journal of International Law,* 52(3), 2012, p. 483-551, at p. 495.

673 ICJ, *Armed Activities in Territory of Congo, op. cit.,* in separate opinion of judge Kooijmans, pars. 26-30, and judge Simma, pars. 7-12.

674 See COUZIGOU, I, "The fight against…", *op. cit*., p. 89; and TRAPP, K. N., "Can non-State actors mount to an armed attack", in WELLER, M., *et al*. (eds.), *The Oxford handbook of the use of force in International Law*, CUP, 2015, p. 679-696, at p. 695.

> response to an "armed attack" as long as that force is necessary and proportionate"[675].

According to this position, in practice, international community accepted the use of the right of self-defence against activities of non-State actors inside another State's territory if the host State is *unable* or *unwilling* to repel non-State actors' activities in its territory[676].

This view is posed to overcome attacks by non-State actors that reside in the territory of another State and they use the State sovereignty as a shield to deter retaliation of victim State[677]. Then, States that suffered an attack seek to pierce host States' shields of sovereignty by resorting to the *unwilling* and *unable* test as practical means to resolve these tensions.

However, one thing is the duty to repress the terrorist groups and another, as the theory of unwilling or unable test pretends, to take it to its ultimate consequences, even by allowing the use of force in its territory and without its consent[678].

In this sense, it is worth mentioning the ICJ view on the *Armed activities in the territory of Congo* where, relating to the question of whether the DRC breached its duty of vigilance by tolerating anti-Ugandan rebels on its territory, the Court affirmed that

> "During the period under consideration both anti-Ugandan and anti- Zairean rebel groups operated in this area. Neither Zaire nor Uganda were in a position to put an end to their activities. However, in the light of the evidence before it, the Court cannot conclude that the absence of action by Zaire's

[675] UNGA, Doc. A/HRC/14/24/Add.6 "Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston", 28 May 2010, par. 32, p. 11-12.

[676] TAMS, C. J.; DEVANEY, J, G., "Applying necessity…, *op. cit.*, p. 100; see also ORR, A. C., "Unmanned, unprecedented, and unresolved: The status of American drone strikes in Pakistan under International Law", *Cornell International Law Journal*, *44*(3), 2011, p. 729-752, at p. 736. NOLTE, G.; RANDELZHOFER, A., "Article 51", *op. cit.*, p. 1418-1419; and ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 12.

[677] WILLIAMS, G. D., "Piercing the shield of sovereignty: an assessment of the legal status of the unwilling or unable test", *University of New South Wales Law Journal*, 36, 2013, p. 619-641, at p. 619-620.

[678] CERVELL, M. J., "Sobre la doctrina <unwilling or unable State>...", *op. cit.*, p. 83-84.

> Government against the rebel groups in the border area is tantamount to "tolerating" or "acquiescing" in their activities. Thus, the part of Uganda's first counter-claim alleging Congolese responsibility for tolerating the rebel groups prior to May 1997 cannot be upheld"[679].

Moreover, in relation to a subsequent period, it stated that

> "The DRC was thus acting against the rebels, not in support of them. It appears, however, that, due to the difficulty and remoteness of the terrain discussed in relation to the first period, neither State was capable of putting an end to all the rebel activities despite their efforts in this period. Therefore, Uganda's counter-claim with respect to this second period also must fail"[680].

Thus, the inability to put an end to irregular activities of the rebel groups does not constitute a violation of the prohibition of the use of force and, consequently, it is not possible to exercise the right of self-defence by a victim State, due to the absence of any armed attack.

In this direction, some authors emphasize that in contemporary International Law there is not any right of self-defence, or at least none under discussion, against non-State actors in the territory of a host State when this State is *unwilling* or *unable* to deal with such actors[681]. They emphasize that even if the host States violated their duty to suppress, for instance, terrorist activities, this cannot justify the right of self-defence against the harbouring State[682]. Nevertheless, while in State practice it seems that States have increasingly come to accept the self-defence in these cases[683], in reality, most of such cases

---

[679] ICJ, *Armed Activities in Territory of Congo, op. cit.,* par. 301.

[680] *Ibid*, par. 303.

[681] Among others, see COUZIGOU, I, "The fight against…", *op. cit*., p. 96; CORTEN, O., "The 'unwilling or unable' test: has it been, and could it be, accepted?", *LJIL,* 29, 2016, p. 778-799, at 778-779; O'CONNELL, M. E., "Adhering to law and values against terrorism", *Notre Dame Journal of International & Comparative Law*, 2(2), 2012, p. 289-304, at p. 301; ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 12; and CERVELL, M. J., "Sobre la doctrina <unwilling or unable State>...", *op. cit*., p. 88-89.

[682] WATERS, Ch., quoted in REINOLD, Th., "State weakness…", *op. cit*., p. 256; and MARAUHN, Th.; NTOUBANDI, Z. F., "Armed conflict, non-international", *op. cit*., p. 68.

have been reactions against the *Daesh.* Thus, this practice can only be seen as the last resort in specific and extreme circumstances of necessity and should not be generalized[684].

In order to repel armed attacks by non-State actors from the territory of another State, there is unanimity in the priority of host State action. In the case that this State is unable to suppress attacks by non-State actors, then the Victim State in each case should obtain the consent by the host State and explore if there is an opportunity to work cooperatively with the territorial State to repress the threat[685]. Thus, the preference of a Victim State must get consent or cooperation with the host State, instead of acting unilaterally.

2. *Proportionality*

Although proportionality was already part of customary International Law[686], it was not included in the UN Charter. The UN Charter recognized the existence of the right of self-defence, but it

> "does not go on regulate directly of its aspects of its content. For example, it does not contain any specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary International Law […]. It cannot therefore be held that article 51 is a provision which 'subsumes and supervenes' customary International Law" [which] "continues to exist alongside treaty law. The areas governed by the two sources of law thus do not overlap exactly, and the rules do not have the same content"[687].

---

[683] REINOLD, Th., "State weakness…," *op. cit*., p. 257; see also ZEMANEK, K., "The prohibition to use force after sixty years of abuse", in BUFFARD, I., *et al*. (eds.), International Law between universalism and fragmentation: in honour of Gerhard Hafner, Nijhoff, 2008, p. 287- 316, at p. 296, where asserts that "it is more credible that during that stage of the evolution of International Law self-defence was considered a reflex rather than a legal right".

[684] CERVELL, M. J., "Sobre la doctrina <unwilling or unable State>...", *op. cit*., p. 89; *Tallinn Manual, op. cit*., rule. 33.

[685] DEEKS, A. S., "'Unwilling or unable'....", *op. cit*, p. 520.

[686] BROWNLIE, I., *International Law…, op. cit*., p. 279.

[687] ICJ, *Nicaragua case, op. cit*., par. 176.

Then, we can assert that the right of self-defence is regulated by customary International Law and by the UN Charter ("This dual condition applies equally to article 51 of the Charter, whatever the means of force employed")[688], and is generally accepted that article 51 inclines to cover all features of the right of self-defence without formally expressing these aspects in a conventional nature[689]. Therefore, proportionality is incorporated in article 51 of the UN Charter.

Proportionality in customary law is traced back to diplomatic deliberations of *Caroline* incident in 1837 which provided the explicit criteria of right of self-defence. The ICJ reflects proportionality as criteria to restrict the exercise of self-defence[690]; however, the concept of proportionality is certainly confusing. In the *Caroline case,* proportionality requirement is illustrated as "[…] nothing unreasonable or excessive […]"[691] which is limited in necessity. Likewise, the ICJ confirmed this rule of customary International Law by the expression that the use of force in self-defence "must be proportional to the armed attack and necessary to respond to it"[692]. From the first glance to the ICJ view, we can infer that the level of use of force in self-defence is not greater than what is necessary to avert armed attack or to eliminate a threat.

a) *Inter-State proportionality*

In relation to the content of the principle of proportionality in International Law, although, the ICJ frequently remarks the criteria of proportionality, it did not constitute a general theoretical network on its content[693]. It seems that in this aspect the Court has been reluctant to define or to offer a clear analysis of dimensions of proportionality in the right

[688] ICJ, *Legality of nuclear weapons, op. cit*., par. 41.

[689] VAN STEENBERGHE, R., "Self-defence...", *op. cit*., p. 186.

[690] ICJ, *Nicaragua case, op. cit*., pars. 176 and 194; *Legality of nuclear weapon, op. cit*., par. 41; and *Oil Platforms* case, *op. cit*., pars. 43, 73, 74 and 76.

[691] Noted by Mr Webster to Mr Fox on 24 April 1841 in DAMROSCH L. F., *et al., International Law..., op. cit.,* p. 923.

[692] ICJ, *Nicaragua case*, *op. cit*., par. 176; and *Legality of nuclear weapon*, *op. cit*., par. 41.

[693] "Equally, since the preconditions for the exercise of self-defence do not exist in the circumstances of the present case, the Court has no need to enquire whether such an entitlement to self-defence was in fact exercised in circumstances of necessity and in a manner that was proportionate", ICJ, *Armed activities on the territory of the Congo , op. cit.,* par. 147.

of self-defence. Today, all States have accepted proportionality requirement as significant factor in the right of self-defence[694].

According to Brownlie, proportionality can be described as the *essence of self-defence*[695]*.* There are two approaches in the interpretation of the criteria of proportionality which are well-known as *double proportionality*[696]. Firstly, favoured by the ICJ, according to proportionality criteria, the use of force in self-defence depends on the size and the scope of the armed attack. In this view, proportionality should be assessed by taking into account the scale of the whole operation (size and scope) as well as necessity of the measures to respond to the attack[697]. Secondly, favoured by some ICJ judges[698]and scholars[699], the proportionate response is to repel the attack in order to restore the situation. In fact, double proportionality essentially combines the two interpretations of proportionality[700].

Also, the accumulation of events theory is applicable to recognize the lawful level of the use of force in self-defence against an offender. In this regard, defender does not need to consider one specific incident[701]. The amount of self-defence operation is determined *as a*

---

[694] IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., p. 99; and GARDAM, J., "Proportionality and force in International Law", *AJIL,* 87(3), 1993, p. 391-413.

[695] BROWNLIE, I., *International law…, op. cit.*, p. 389.

[696] CHRISTODOULIDOU, T.; CHAINOGLOU, K., "The principle of proportionality from a *jus ad bellum* perspective", in WELLER, M. *et al*. (eds.), *The Oxford Handbook..., op. cit.,* p. 1187-1208, at p. 1192.

[697] ICJ, *Nicaragua case, op. cit*., par. 176; and *Oil Platforms case*, *op. cit*., par. 72.

[698] ICJ, *Nicaragua case, op. cit.,* dissenting opinion of judge Schwebel, pars. 211–214; ICJ, *Legality of nuclear weapons*, *op. cit*., dissenting opinion of judge Higgins, par. 5; and ICJ, *Armed activities in territory of Congo, op. cit.,*separate opinion of judge Kooijmans, pars. 33 and 34.

[699] GARDAM, J., "'Proportionality...", *op. cit*., p. 403; GREENWOOD, Ch., "Self-defense and the conduct of international armed conflict" in DINSTEIN, Y.; TABORY, M. (eds.), *International Law at a time of perplexity. Essays in honour of Shabtai Rosenne*, Martinus Nijhoff, 1989, p. 273-288, at p. 273; and CORTEN, O., *The law against war.., op. cit.,* p. 489.

[700] CHRISTODOULIDOU, T.; CHAINOGLOU, K., "The principle of proportionality...", *op. cit*., p. 1193; and OCHOA, R. N.; SALAMANCA-AGUADO, E., "Exploring the limits of International Law relating to the use of force in self-defense", *EJIL*, 16(3), 2005, p. 499-524, at p. 520.

[701] *The Chatham House principles*…", *op. cit*., p. 969; and ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 4.

whole; the ICJ in *Oil platforms* case by assessing proportionality mentioned that it "could not close its eyes to the scale of the whole operation"[702].

In the practice, all action in self-defence, according to International Law, must respect three criteria: first, the defensive action does not have to be in relation with the means used by the attacker, but with the purpose of defending the territory. This concept derives from the ICJ's view which mentions that proportionate response in the right of self-defence amounts to any kind of measure necessary to repel the armed attack[703].

Second, a proportionate action is limited to the defensive purpose (should not be oriented to other purposes); that is, the response must be proportionate to the attack and must be compatible to the purpose of the self-defence. In other words, response in self-defence must not exceed the amount of necessity sufficient to defend against the armed attack received; then, it must not serve as an excuse to start a large-scale attack. The action in self-defence must be provided based on the nature and intensity of the attack and sufficient to deactivate it[704]. The proportionality refers to the *quantum* of force that the victim State is authorized to use to repel the *quantum* of aggressor's force, and it is according to the type of committed force and purpose of the self-defence; this does not mean an identity in the material means used by the attacker and defendant. In fact, the matter is not the kind of means employed, but the goal pursued by the current defence of the State. The immediate nature of the response, necessity and proportionality are conditions that must be assessed case-by-case based on the circumstances of each particular case[705]. The proportionality requirement is not a static legal formality; it is determined in accordance with certain extent of hostilities, duration of military operation, choice of mean and methods of conflict, or geographical operations.

---

[702] ICJ, *Oil platforms case*, *op. cit*., par. 77.

[703] ICJ, *Nicaragua case*, *op. cit*., par. 194.

[704] TRAPP, K. N., "Back to basics...", *op. cit.*, p. 141 and 146.

[705] CASANOVAS, *O., "El principio…", op. cit*., p. 1073.

A general rule to measure proportionality is that, in the face of two equally defensive measures, one should prefer the less injurious measure to the attacker, which in practice is not easy to determine. Defender must use the least harmful action against the attacker and it cannot make unnecessary damages to it. Thus, proportionality does not allow to *punish* the attacker, but at the same time, such concept does not infer that there must be equality between response in self-defence and the harm of the attack either already suffered.

In this context, we can consider dangerous the view that response in self-defence may occur with greater intensity than initial armed attack. This idea was implied in *Falklands-Malvinas* conflict in 1982, when during the use of self-defence by British led to the loss of 907 lives *versus* none lives lost during the Argentina invasion, and this was not seriously considered disproportionate[706]. In this regard, it is interesting to refer to Rule 14 *proportionality in attack* of the International Committee of Red Cross (ICRC) which mention that even in the case of warfare "launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited"[707].

In the third criteria, one of the limits to the right of self-defence is the territory of the other State; however, in the case that the conflict continues in the border area, the defending State may temporarily penetrate into the territory of the attacker in order to defend itself[708]. The temporary penetration into the alien territory by the defender must end at the moment when the aggressor stops using armed force.

In addition to these criteria, in some cases we must observe that the remoteness of action in self-defence, according to the nature of the original attack, can violate the principles of proportionality and necessity[709]. As the ICJ confirmed, "The Court cannot fail to observe,

---

[706] TAMS, C. J.; DEVANEY, J. G., "Applying necessity…, *op. cit*., p. 102,

[707] ICRC, *Rules of International Humanitarian Law and other rules relating to the conduct of hostilities*, of 20 June 2005.

[708] See KITTRICH, J., *The right of individual self-defence..., op. cit.,* p. 23.

[709] CHRISTODOULIDOU, T.; CHAINOGLOU, K., "The principle of proportionality...", *op. cit*., p. 1191.

that the taking of airports and towns many hundreds of kilometres from Uganda's border would not seem proportionate to the series of transborder attacks it claimed had given rise to the right of self-defence, nor to be necessary to that end"[710].

In anticipatory self-defence, where proportionate reaction is not limited to repel an attack that has taken place, the response may apply to avert imminent armed aggression[711]. In any case, the amount of physical and economic consequences of force must not exceed the harm expected from the attack[712]. In this sense, according to the proportionality requirement, a balance is requested between the capacity of the State to use any means necessary to defend its territory, and the survival of the principle of non-use of force which does not allow a truly defensive action to be transformed into an aggression.

As the last resort, the right of self-defence will be controlled by the UNSC, which must take all circumstances into consideration. Proportionality is a valid principle influenced in the UNSC and has been widely evidenced in practice as well as in the opinion of the States throughout the functioning of the Council. However, the objective appreciation of proportionality is complex. The reality is that the answers in presumed self-defence against attackers are often characterized by their lack of proportionality. The UNSC, in some resolutions, has reflected the excessive character of use of force[713].

It is worth finding out whether an act of self-defence without proportionality requirement has the same sanction as an aggression. In this regard, there is no practice but we need to look for an equitable solution. In principle, one action in self-defence following necessity and immediacy criteria but without respecting the proportionality will not be serious as an

---

[710] ICJ, *Armed activities on the territory of the Congo , op. cit.,* par. 147.

[711] MURPHY, S. D., "The Doctrine of pre-emptive self-defence", *Villanova Law Review*, 50(3), 2005, p. 699-748, at p. 735; and SCHMITT, M. N., *Counter –terrorism..., op. cit.,* p. 20.

[712] *The Chatham House principles*…", *op. cit*., p. 969.

[713] For instance among others, UNSC, Resolutions 248, 256 and 262 in relation to Israel military action on territory of Jordan in 1968; Resolutions 509, 512, 513 and 515 in regard to Israel military assault to Lebanon in 1982; Resolutions 568 and 571 in concern to military attacks by south Africa against Botswana 1985; UNSC, Resolution 582 in relation to conflict between Iraq-Iran in 1986, UNSC Resolution 1397 on Israel-Palestine in 2002; See, also UNSC, Resolution 1701 on the full cessation of Israel bombing to Hezbollah in Lebanon, 11 August 2006.

act of aggression, because: i) the aggression involves the use of armed force against a State in situation of peace; to the contrary, the self-defence is an act responding to an unfair attack; ii) it is not found in the cases of article 3 of the Resolution 3314 (XXIX); iii) the majority of domestic regulations, mitigated penalty for acts committed in excess of defence; iv) the different nature of the requirements; while necessity or immediacy are a matter of all or nothing, the appreciation of the proportionality will always be a degree of trial; v) the nature of defensive military operations itself makes difficult to determine the proportionality; an act in self-defence means the use of armed force and, in military plans, concepts, such as the measure, cannot be taken into account directly; and vi) Iran's declarations in his conflict with Iraq vividly shows that excessive defence may be an understandable cause, from the point of view of all States, of the insufficiency of collective security system of the UN[714].

We must recognize that it is very difficult to accept a stopping hostility in self-defence when serious doubts are raising about the reality of reparation by aggressor. Hence, the State that acts in self-defence is leaning more towards obtaining its right rather than what the international order will hardly give it.

Therefore, the responsibility of who violated the principle of the prohibition of the use of force is not equated with who exceedingly (no proportionally) acted in self-defence (necessity and immediacy).

Another interesting issue is whether the States have the authorization to use nuclear weapons or any other weapons of mass destruction (WMD) in the right of self-defence. The ICJ in the *Legality of nuclear weapons* merely stated that

> "in view of the current State of International Law, and of the elements of fact at its disposal, the Court cannot conclude definitely whether the threat or use

[714] See ORTEGA, M. C., *La legítima defensa…, op. cit.,* p. 131-137.

of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of State would be at stake"[715].

In fact, the Court only affirmed that "the threat or use of nuclear weapons would generally be contrary to the rules of International Law applicable in armed conflict, and in particular the principle and rules of humanitarian law"[716].

The nearly absolute silence of the ICJ does not exclude that a negative response can be given based on the catastrophic effects of WMD, which would make it very difficult to justify proportionality, unless the previous attack had also used the atomic weapon. However, even in the latter case, it must be understood that its use would be contrary to humanitarian law[717].

Nevertheless, when the ICJ says *generally* is because it is aware that there may be elements that may entail the agonizing prevalence of the State's interest in its survival over humanitarian principles. In this sense, the ICJ considers that it does not have all the sufficient elements to assert with certainty that the use of nuclear weapons is necessarily contrary to the principles and rules of the law applicable to the armed conflicts in any circumstance, since it cannot ignore the fundamental right of the State to survival[718]. However, when a victim State (and its allies) consider that they do not have sufficient forces against a very powerful occupant, then maybe it is better not to act to avoid a widespread conflict[719].

---

[715] ICJ, *Legality of Nuclear weapons*, *op. cit.*, par. 106-E; this paragraph was adopted thanks to the vote of President Bedjaoui's quality; see also pars. 95-97.

[716] *Ibid.*

[717] GONZALEZ, J. D., *et al*., *Curso…, op. cit*., p. 1019.

[718] ICJ, *Legality of nuclear weapon, op. cit.,* par. 96-97; and REMIRO, A., *et al*., *Derecho Internacional, op. cit*., p. 679.

[719] See ORTEGA, M. C., *La legítima defensa…, op. cit.,* p. 89.

b) *Proportionality and non-State actors*

In relation to what does proportionality response in the right of self-defence against non-State actors mean, recent State practice in use of self-defence against non-State actors in the territory of another State, "seems to have exacerbated proportionality's conceptually weak condition"[720]. In this regard, we have to point out, firstly, the recent international practice in the use of force in self-defence which indicates that response in self-defence can *pursue far-reaching aims*. For example, broad reaction by Israel against Hezbollah in 2006 to weaken such non-State actor, and Turkey's operation against PKK in the North of Iraq in 2008, went beyond what was necessary to repel or avert the attacks[721]. Likewise, US self-defence operation in Sudan and Afghanistan was more *punitive rather than defensive*[722]. Hence, there are serious debates about models of self-defence and whether a proportionate response is limited only to repel an armed attack or rather to eliminate future attacks. The answer to this question is difficult but it appears that if a response in self-defence has been carried out to weaken the non-State actor (wider aim), then the use of an excessive level of force in comparison to that wider aim would be disproportionate[723].

Secondly, the recent State practice in the exercise of the right of self-defence against non-State actors stretch the temporal limits to the use of force, particularly when the accumulation of events theory authorize response against series of small attacks, since such theory undermines the temporal concept of self-defence[724]. For instance, cumulative proportionality approach is related to the case of series of attacks targeting a State. In this context, States, annoyed by threats or attacks on a repetitive basis by a non-State actor, may only have one chance to repel future attacks or to reduce their frequency and effectiveness. Therefore, the victim State has the right to exercise the use of force in a

[720] TAMS, C. J.; DEVANEY, J. G., "Applying necessity…", *op. cit*, p. 102.

[721] *Ibid*, p. 103; see also TRAPP, K. N., "The Turkish intervention against the PKK...", *op. cit*., p. 700.

[722] GRAY, C., *International law..., op. cit.,* p. 205; CANNIZZARO, E.; RASI, A., "The US strikes in Sudan and Afghanistan-1998", in RUYS, T.; *et al*. (eds.), *The use of force..., op. cit.,* p. 541-551, *at* p. 545-546.

[723] TAMS, C. J.; DEVANEY, J. G., "Applying necessity…, *op. cit*., p. 103.

[724] *Ibid*.

greater degree to every non-State actors' attacks to eliminate the centre of its organization[725].

Despite the complexities to clarify proportionality criteria in self-defence against non-State actors, it is inevitable to dismiss the role of proportionality factor in self-defence or envisage proportionality criteria as a rhetorical tool[726].

The international practice evaluates some general principles on proportionate response on self-defence against armed attack by non-State actors: first, the essential effect of self-defence must be to repel ongoing attacks and prevent future situations to pursue an armed attack[727]. In the case of Turkey against PKK in 2008 and Israel against Hezbollah in 2006 they show that responses in self-defence were carried out to repel or avert the attack and aimed to weaken the non-State actors. As we have seen *supra,* the international community did not complain.

Second, the recent State practice shows that States usually supported *quantitative concept* of proportionality. According to proportionate response in self-defence, reaction request "a balance between the damages caused and military means used by the attackers and the damages caused and military means used by State in self-defence"[728]. In this field, Israel operation in front Hamas in 2006, exceeded what was necessary when attempted to achieve other objectives such as the destruction of Lebanon economy or the elimination of Hamas[729].

Third, it seems there is no great concern when victim States exceed the harm to non-State actors than damage inflicted to a victim State. This concept was inferred from Turkey's response in self-defence against PKK in 2008, where casualties were 20 times higher than

[725] CHRISTODOULIDOU, T.; CHAINOGLOU, K., "The Principle of proportionality...", *op. cit*., p. 1200.

[726] GARDAM, J. G., *Necessity, proportionality..., op. cit.,* p. 187.

[727] CORTEN, O., *The law against war*...,*op. cit*., p. 485; and PERT, A., "Proportionality in self-defence–proportionate to what?", *Pandora Box*, 24(17/95), 2017, p. 65-78, at p. 78.

[728] VAN STEENBERGHE, R., "Self-defence...", *op. cit*., p. 205.

[729] *Ibid*, p. 206; TOMAS, C.; BRUCKNER, W., "The Israeli intervention in Lebanon...", *op. cit*., p. 674.

Turkey's, but the scale of invasion was not seen excessive by the States' view[730]. This approach indicates that in some circumstances, response in the right of self-defence can be little more intense rather than initial armed attack by non-State actors[731].

Forth, the aim of the self-defence is to end ongoing danger. Hence, proportionality is defined to achieve this legitimate aim[732]. ILC affirmed that

> "it would be mistaken, however, to thinks that there must be proportionality between the conduct constituting the armed attack and the opposing conduct. The action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered. What matters in this respect is the result to be achieved by the 'defensive' action, and not the forms, substance and strength of the action itself"[733].

Fifth, there is not a geographical limitation to respond in self-defence. Reaction can target non-State actors at their base even far-away[734]. The geographical scope may be expanded in the proportionate response in self-defence against non-State actors in the territory of other State; for instance, drone attacks in cross border operations[735]. When the territory of a State is being used by non-State actors and such host State is unable to react sufficiently to avoid that, by exercising the last resort in specific extreme situations of necessity, both military units or military drones defending States can cross the border of the host State without its consent with the purpose of eliminating the threat. As soon as the threat is eliminated, military units or military drones must leave the territory of the host State. It is not lawful to deploy military force in a location void of targeted non-State actors[736]. For

---

730 TAMS, C. J.; DEVANEY, J. G., "Applying necessity…", *op. cit*, p. 104.

731 *Ibid.*

732 LUBELL, N., *Extraterritorial..., op. cit.,* p. 65.

733 ILC, "State responsibility", *op. cit.,* vol. ll, part 1, 1980, par, 121.

734 TAMS, C. J.; DEVANEY, J. G., "Applying necessity…", *op. cit*, p. 104; and KITTRICH, J., *The right of individual self-defence..., op. cit.,* p. 27.

735 SCHACHTER, O., *International Law in theory and practice*, Martinus Nijhoff, 13, 1991, p. 154.

736 SCHMITT, M. N., "Drone attacks under the *jus ad bellum* and *jus in bello*: clearing the 'fog of law'", *Yearbook of International Humanitarian Law,* 13, 2010, p. 311-326, at p. 317.

instance, response in self-defence may be used to neutralize terrorist cells, destroy terrorist training camps engaged in hostile activities, with the purpose of reducing their capacity to plan, organize and launch more attacks[737].

Sixth, a general principle of International Law is that response in self-defence must only target non-State actors[738]. There is an excessive use of force in self-defence (disproportionate) if it directly targets host States instead of non-State actors[739]. This concept is inferred from the reaction of international community against Israeli attack to Beirut airfield in Israel-Hezbollah conflict in 2006[740].

And seventh, in light of the proportionality, any operation in self-defence against a non-State actor must prevent civilian suffering. This concept implicitly came from Israeli military intervention in Lebanon in 2006 and Gaza during 2008-2009 when international community criticized the use of self-defence as a *lacking focus* which led to casualties of civil population in the host State. These are appropriate examples of violation of the proportionality requirement where they have been unanimously condemned because of their disproportionate nature[741].

---

[737] GAZZINI, T., *The changing rules on the use of force..., op. cit.,* p. 198.

[738] O'CONNELL, M. E., *The power ..., op. cit.,* p. 181

[739] TAMS, C. J.; DEVANEY, J. G., "Applying necessity…", *op. cit*, p. 105.

[740] Among others, see Argentina, UNSG and Russian Federation views in UNSC, Doc. S/PV.5489, on "the situation in the Middle East", 30 July 2006.

[741] In regard to the Israel intervention in Lebanon, see Russia, UN Doc. S/PV.5489, at 7; Argentina, UN Doc. S/PV.5489, at 9; Qatar, UN Doc. S/PV.5489, at 10; China, UN Doc. S/PV.5489, at 11; Japan, UN Doc. S/PV.5489, at 12; Greece, UN Doc. S/PV.5489, at 17; France, UN Doc. S/PV.5489, at 17; Congo, UN Doc. S/PV.5489, at 13; Tanzania, UN Doc. S/PV.5489, at 13; Ghana, UN Doc. S/PV.5493 (resumption 1) at 8; Brazil, UN Doc. S/PV. 5493 (Resumption 1) at 19 and New Zealand, UN Doc. S/PV.5493 (resumption 1) at 33; also in regarding to Israel intervention in Gaza, see South Africa, UN Doc. S/PV.6060, at 9; Indonesia, UN Doc. S/PV. 6060, at 10; Belgium, UN Doc. S/PV.6061, at 17; Mexico, UN Doc. S/PV.6061, at 19: Argentina, UN Doc. S/PV.6061 (Resumption 1) at 8; Pakistan, UN Do. S/PV.6061 (Resumption 1) at 10; Turkey, UN Doc. S/PV.6061 (Resumption 1) at 10; Iceland, UN Doc. S/PV.6061 (Resumption 1) at 15; Ecuador, UN Do. S/PV.6061 (Resumption 1) at 16; Bolivia, UN Doc. S/PV.6061 (Resumption 1), at 17; Paraguay, UN Doc. S/PV.6061 (Resumption 1) at 17; Vietnam, UN Doc. S/PV.6060, at 17; Egypt, UN Doc. S/PV. 6060, at 18 and Costa Rica, UN Doc. S/PV.6060, at 16.

3. *Immediacy*

In principle, the armed response under the right of self-defence can only be carried out against a current and effective armed attack and always *a posteriori* of the onset of the attack by other State. In this section, we are going to find out the meaning and scope of the term immediacy in the context of the right of self-defence. If an action in the right of self-defence does not meet the requirement of immediacy to respond to the attack, then the exception cannot be applicable. In principle, the foundation is the same as the lack of necessity: the force is no longer used to counter attack but rather for other purposes.

a) *Concept of immediacy*

In order to justify the right of self-defence, States must meet immediacy alongside other requirements, which are closely related with the necessity[742]. As the ILC affirmed

> "There remains the third requirement, namely that armed resistance to armed attack should take place *immediately,* i.e. while the attack is still going on, and not after it has ended. A State can no longer claim to be acting in self-defence if, for example, it drops bombs on a country which has made an armed raid into its territory after the raid has ended and the troops have withdrawn beyond the frontier"[743].

In fact, the lack of immediacy cannot be differentiated from the lack of necessity. The action of self-defence must overlap in light of the time with a wrongful attack; in other words, the defensive action must be current, that is, it must occur at the same time of the attack.

The self-defence must consist of immediate response in time and space to aggressive action, since the use of force in self-defence is justified only to the necessary extent to counteract the attack. Otherwise, the self-defence would be transformed into an armed retaliation that is prohibited by article 2(4) of the UN Charter. This would be the case of US air raids against Iranian oil platforms in the Persian Gulf, where other conditions were also

[742] ICJ in *Nicaragua case op. cit.*, implicitly commented that necessity-coupled with the condition of immediacy, par 237; see also DINSTEIN, Y., War, aggression..., *op. cit.*, p. 299.

[743] ILC, "State responsibility", *op. cit.*, vol. II, part 1, 1980, p. 70.

violated. In this sense, the requirement of immediacy distinguishes the use of force under the right of self-defence from mere retaliation[744]. In this regard, the temporal proximity factor is necessary between attack and response[745]. Also, it is interesting to point out that the reaction to an armed attack must be immediate and excludes the necessity of a formal declaration of war, which may be subject to long internal procedures[746].

The majority of the ICJ judgements just repeated other requirements of the right of self-defence, but immediacy has not been expressly recognized by the ICJ[747]. However, its existence is confirmed in customary International Law in the *Caroline case* in 1837 when necessity, proportionality and immediacy are the three conditions that were distilled by the American Secretary D. Webster.

In relation to the *beginning of attack*, normally in practice, the UNSC denies the right of self-defence when the attack is ready to occur. When facing imminent attacks, States either inform the UNSC or do not take any action. Premeditated operations do not meet the requirements of immediacy (and necessity).

However, temporal immediacy should not be judged in absolute terms. The immediacy must be considered based on the time that is necessary to prepare the armed response, the subsistence of the attack or the foreign occupation of the territory and the possibilities that can give the collective security system[748]. In this sense, sometimes in the UNSC, it has arisen the idea that immediacy not only refers to the time, but also to the space *immediately*

[744] VACAS, F., *El régimen jurídico del uso de la fuerza por parte de las Operaciones de Mantenimiento de la Paz de Naciones Unidas*, Marcial Pons, 2005, p. 248.

[745] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 12.

[746] PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 666.

[747] IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., p. 117.

[748] REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 680.

and in the same location in relation to the attack[749]. In fact, nowadays due to the complexity of conflicts, it is advisable a flexible interpretation of the immediacy requirement[750].

b) *Preventive self-defence is unlawful*

According to the UN Charter, contrary to the imminent threat already covered by article 51, other latent that are not imminent threats are under the authority of the UNSC to use military force to preserve international peace and security[751].

Literally, although all terms (preventive, pre-emptive, and anticipatory self-defence) refer to the use of force *prior* occurring an armed attack, in International Law there is a distinction between them in light of imminent threat. In this field, there are rhetorical distinctions among scholars to address the right of self-defence against threat and *imminent* threat. For instance, often pre-emptive and anticipatory self-defence are used to refer to the same concept[752], while preventive self-defence is used to refer to another concept. However, this rule is not followed by some authors that literally made distinctions between pre-emptive and anticipatory self-defence. For instance, Murphy claims that "Pre-emptive self-defence is used to refer to the armed coercion by a State to prevent another State or (non-State actors) from pursuing a course of action that is not yet directly threatening" [753]. In our view, preventive self-defence is used with relation, in general, to attacks not consummated. However, it is necessary to distinguish between anticipatory

[749] See GREENWOOD, Ch., "Self-defence...", *op. cit*., p. 276; and ORTEGA, M. C., *La legítima defensa…, op. cit.,* p. 97-98.

[750] CERVELL, M. J., *La legítima defensa..., op. cit*., p. 142.

[751] UNGA, Doc. A/59/2005, Secretary-General's report "In larger freedom: towards development, security and human rights for all", 21 March 2005, pars. 124-125; see also *The Chatham House principles*…, *op. cit*., p. 971.

[752] PÉREZ, M., "La legítima defensa puesta en su sitio: observaciones críticas sobre la doctrina Bush de la acción preventiva", *REDI*, 55 (1), 2003, p. 187-204, p. 199.

[753] MURPHY, S. D., "The doctrine of pre-emptive…", *op. cit.,* p. 704; see also DEEKS, A. S., "Taming the doctrine of pre-emption", in WELLER, M.; *et al.* (eds.), *The Oxford handbook of the use of force in International Law,* OUP, 2015, p. 661-678, at p. 666; and US, DoD, OFFICE OF GENERAL COUNSEL, *Legal Distinction...,op. cit.*

self-defence when the attack is imminent (high probability that occurs) and pre-emptive self-defence[754] when the attack is latent (the probability is farther in the time).

Actually, in 2002, G. W. Bush set out the new strategic doctrine of preventive self-defence[755]. In accordance with this doctrine, the global international terrorism and the proliferation of nuclear weapons are new threats that demand a policy of preventive actions to protect the national security of the US. When

> "the greater the threat, the greater is the risk of inaction— and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act pre-emptively"[756].

British government explicitly expressed its opposition to US doctrine on preventive action which set out in the US *National Security Strategy*. In this context, Lord Goldsmith mentioned "it is therefore the Government's view that International Law permits the use of force in self-defence against an imminent attack but does not authorise the use of force to mount a pre-emptive strike against a threat that is more remote"[757].

As is mentioned *supra*, the authors who support an extensive interpretation of the right of self-defence are based on the fact that the right of self-defence (inherent right) refers to the customary nature prior to article 51 of the UN Charter. These authors argue that at the time of the adoption of the Charter there was a broad customary right of self-defence that

---

[754] US, *The National Security Strategy of the United States,* The White House, September 2002, available at https://www.state.gov/documents/organization/63562.pdf, [visited on 23 February 2018]. It used the term *pre-emptive self-defence* to refer to attacks not strictly imminent, p. 15.

[755] LEVY, J. S., "Preventive war and democratic politics", *International Studies Quarterly* 52(1), 2008, p. 1-24, at p. 16; see also OBAYEMI, O. K., "Legal standards governing pre-emptive strikes and forcible measures of anticipatory self-defence under the UN Charter and General International Law*", Annual Survey of International Law and Comparative Law*, 12, 2006, p. 19-42, at p. 23 and 29.

[756] US, *The National Security Strategy of the United States,* The White House, September 2002, p. 15, *op. cit.*; see also PÉREZ, M., "La legítima defensa…", *op. cit.*, p. 187-204.

[757] GOLDMITH, L., Attorney General of the UK, House of Lords, *Hansard*, 21 April 2004, column 370.

allowed the protection of nationals abroad and the preventive self-defence[758]. Thus, this doctrine assumes that in customary International Law, preventive self-defence was allowed to confront threats[759].

Consequently, the right of self-defence against an armed attack would only be one of the forms of self-defence which are allowed by the Charter. Another form would be the preventive self-defence[760].

Regarding the position of a sector of the Anglo-saxon doctrine that defends the lawfulness of self-defence in cases of *threat or imminence* of an armed attack, the dominant tendency has indicated that it is highly controversial that the *Webster formula*[761]of the preventive self-defence has survived the Charter[762].

This current doctrine states that if the UN Charter does not say "only if an armed attack occurs" neither does add "or threatens". For this reason, it understands that the self-defence does only come up when an armed attack exists. The limits imposed on self-defence in article 51 of the UN Charter would be meaningless if a broader customary law was preserved[763]. In addition, they point out that prior to the Charter, customary law only allowed a restrictive right of self-defence[764]; likewise, the possibility of preventative self-defence was debated and rejected, among others, by the US within the framework of the

---

758 GRAY, C., *International Law and the use of force*, OUP, 2004, p. 98.

759 Among others, for example, BOWETT, D. W., *Self-Defence...*, *op. cit*., p. 188-193; WALDOCK, C. H. M., "The regulation...", *op. cit*., p. 463; McDOUGAL, M. S.; FELICIANO, F. S., *Law and minimum world public order: the legal regulation of international coercion*, Yale University Press, 1961, p. 232-241; and PASTOR, J. A., *Curso de Derecho…, op. cit.,* 664.

760 WALDOCK, C. H. M., "The regulation...", *op. cit* p. 497-498.

761 According to Webster doctrine, a requirement to use of force in self-defence is "a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation".

762 BOTHE, M., "Terrorism and the legality of pre-emptive force", *EJIL*, 14 (2), p. 227-240, at p. 231-232; and RIPOL, S., "La nueva doctrina global de la defensa preventiva. Consideraciones sobre su caracterización y fundamento", in GARCIA, C.; RODRIGO, A. (eds.), *El imperio inviable. El orden internacional tras el conflicto de Irak*, Tecnos, 2004, p. 141-164, at p. 145-152.

763 Among others, see BROWNLIE, I., *International law...*, *op. cit*., p. 264; JIMÉNEZ DE ARECHAGA, E., "International Law in the past third of a Century", *RCADI*, 1, 1978, p. 9-343, at p. 96 ; KUNZ, J. L., "Individual and collective...", *op. cit*., p. 878; and BOTHE, M., "Terrorism...", *op. cit*., p. 227-240.

764 GRAY, C., *International Law..., op. cit.,* p. 98.

San Francisco Conference that adopted the UN Charter[765]. Similarly, it should be mentioned that since self-defence is an exception (an exceptional right)[766], "The nation acting in self-defence must act within strict confines"[767]. In this sense, it cannot be argued that there is a concept of self-defence that authorizes preventive self-defence[768].

Most of the European doctrine has argued that the use of force in self-defence "is only admissible in response to an ongoing armed attack and as long as the Security Council is not in a position to intervene to maintain international peace and security. The mere threat of an attack must be reported to the Security Council which is responsible for verifying its existence […] and adopting measures to prevent it"[769].

According to Dinstein, the UN member States are barred from exercising the right of self-defence in response to mere threat of force (not imminent threat); therefore in US-Cuba case when the US imposed a *quarantine* on Cuba in 1962, after the installation of Soviet missile on the island, that could not have been adopted under article 51[770]. Likewise, in Israel–Syria case in 2007 where Israel attacked Syria's nuclear installations, that was not lawful in accordance with the right of self-defence[771]. Thus, despite the hostilities between Israel-Syria (and Iran), it is hard to suppose that ultimately Syria's and Iran's nuclear

---

[765] UNCIO, *Documents of the United Nations Conference on International Organization,* Commission III, Security Council, vol. XI, San Francisco 1945, p. 72-73.

[766] ILC mentioned that "self-defence is to be regarded as an exceptional circumstance precluding the wrongfulness of conduct inconsistent with a general obligation to refrain from the use of force, ILC, "State responsibility", *op. cit.*, 1980, vol. II, part 1, p. 52.

[767] FOLEY, B. J., "Avoiding a death dance...", *op. cit*., p. 139.

[768] TSAGOURIAS, N., "Necessity and the use of force: a special regime", in *Necessity across International Law, NYIL*, 41, 2010, p. 11-44, at p. 17; GRAY, C., "The limits of force", *RCADI*, 376, 2014, p. 113-120; see also REISMAN, W. M.; ARMSTRONG, A., "The past and future of the claim of pre-emptive self-defence, *AJIL*, 100(3), 2006, p. 525-550, at p. 549 and NEUHOLD, H., *The law of international conflict: force, intervention and peaceful dispute settlement*, Brill, 2015, p. 141.

[769] IOVANE, M., DE VITTOR, F., "La doctrine européenne et l'intervention en Iraq", *AFDI,* 49, 2003, p. 17-31, at p. 27; see also SÁNCHEZ, L. I., "Una cara oscura del Derecho Internacional: legítima defensa y terrorismo internacional", *Cursos de Derecho Internacional de Vitoria-Gasteiz*, *2002,* Universidad del País Vasco, 2004, p. 269-299, at p. 281; PÉREZ, M., "La legítima defensa...", *op. cit*., p. 190; and LOWE, V., "The Iraq crisis: what now?", *ICLQ*, 52(4), 2003, p. 866.

[770] DINSTEIN, Y., *War, aggression,…", op. cit.*, p. 226.

[771] RUYS, T., '*Armed attack' ..., op. cit.,* p. 363.

devices would be used against Israel, and as a result preventive self-defence is excluded by article 51[772].

Some authors assert that the right of self-defence had no reason to exist before the UN Charter, since it only makes sense when the use of force is prohibited by article 2(4). Hence, preventive self-defence cannot be invoked based on customary rules prior to the Charter nor the UN Charter. In addition, the practice of the UN supports this position after the UNSC refusal to accept the thesis that any action which is not a response to an armed attack can constitute self-defence[773]. For instance, during Israel airstrike on 7 June 1981 which destroyed the nuclear reactor of Osirak (Iraq), it invoked the right of self-defence, but the UNGA Resolution 36/27 qualified its action as an act of aggression[774] and neither the UNSC nor any State accepted the validity of Israeli excuse[775].

The US and the UK attacks to Afghanistan after September 11 can be defined as preventive self-defence (against an indirect aggression of Afghanistan)[776], nevertheless as we have seen *supra*, important actors (UNSC[777], NATO Council[778] or EU[779]) of international relations seems legitimated their plea.

---

[772] DINSTEIN, Y., *War, aggression,…", op. cit.*, p. 227.

[773] PÉREZ, M., "La legítima defensa...", *op. cit.*, p. 192-193; PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 664; and CERVELL, M. J., *La legítima defensa …, op. cit.,* p. 32-33.

[774] UNGA, Resolution 36/27 on the Armed Israeli aggression against the Iraqi nuclear installations, 13 November 1981.

[775] FISCHER, G., "Le bombardement par Israël d'un réacteur nucléaire irakien", *AFDI*, 27, 1981, p. 147-167, at p. 164; D'AMATO, A., "Israel's air strike upon the Iraqi nuclear reactor", *AJIL,* 77(3), 1983, p. 584-588, at p. 586.

[776] RATNER, S. R,. "*Jus ad bellum* and *jus in bello* after September 11", *AJIL*, 96(4), 2002, p. 905-921, at p. 907; and BYERS, M., "The intervention in Afghanistan-2001", *op. cit.*, p. 636.

[777] UNSC, Resolutions 1368 and 1373 in 2001.

[778] The North Atlantic Council, NATO's policymaking organ, asserted that "if it is determined that this attack was directed from abroad against the United States, it shall be regarded as an action covered by Article 5 of the [1949] Washington Trea-ty", making an attack on one ally an attack on all, and invoked the "commitment to collec-tive self-defence", Statement by the North Atlantic Council, Press Release (2001)124, 12 September 2001, available at https://www.nato.int/docu/pr/2001/p01-124e.htm, [visited on 22 July 2017]; see also RATNER, S. R,., "*Jus ad bellum* and *jus in bello...", op. cit.,* p. 909.

[779] European foreign ministers meeting the next day of the attacks to discuss a joint response, officially expressed solidarity with the United States, see "Reaction from around the world", New York Times, 12

In this context, Pastor believes that they were not facing a case of self-defence because their answer was not against an imminent threat and the UNSC never adopted the necessary measures of article 42 to maintain international peace and security[780]. Similarly, it indicates that while it seemed that a *lex specialis* was being created (legality of preventive self-defence for large-scale terrorist acts), such a possibility was cut by the divergences among the UNSC members (France, Russia and China) and other States with Iraq crisis in 2003[781].

The Report of the High level Panel on threats, challenges and change discussed what happens when the threat is not imminent but is real as it happens, for example, with the acquisition of the nuclear weapons-making capability, for hostile purposes. "The short answer is that if there are good arguments for preventive military action, with good evidence to support them, they should be put to the Security Council, which can authorize such action if it choose to". And the *Report* adds that "those impatient with such a response, the answer most be that, in a world full of perceived potential threats, the risk to the global order and the norm of non-intervention on which it continues to be based is simply too great for the legality of unilateral preventive action, as distinct from collectively endorsed action, to be accepted. Allowing one to so act is to allow all"[782].

The same idea is repeated in the *Report* of the Secretary-General, *In larger freedom: towards development, security and human rights for all*, where it differentiates between imminent threats, where the inherent right of self-defence can be exercised, and latent where "the Charter gives full authority to the Security Council to use of military force,

---

September 2001, available at https://www.nytimes.com/2001/09/12/us/reaction-from-around-the-world.html,]visited on 12 March 2018[.

[780] PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 790; see also MURPHY, S. D., "Assessing the legality of invading Iraq", *Georgetown Law Journal,* 92(2), 2003, p. 173-257, at p. 77.

[781] PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 655 and 790.

[782] UNGA, Doc. A/59/565, *Note [transmitting report of the High-level Panel on Threats, Challenges and Change, entitled "A more secure world : our shared responsibility"],* 2 December 2004, par. 188 -191.

including preventively to preserve international peace and security"[783]. In this sense, *The Chatham House principles* assert that "The Council retains the right and responsibility to authorise collective military action to deal with actual or latent threats"[784]**.** Then, the UNSC is the only one responsible to act preventively in front of latent threats[785].

Therefore, the conception of preventive self-defence as an international political measure of a State does not have place in the Charter[786]. In this regard, Pastor exposes that there are three arguments: first, an interpretation in this sense of article 51 of the UN Charter would blur the boundary between what would be a real preventive self-defence and an armed retaliation which are prohibited by International Law; second, the unilateral uses of force not submitted to any institutional control, easily leading to strategic errors as, for instance, the killing in Afghanistan on 1 July 2002 of forty natives who celebrated a wedding and they made outbursts of joy, that the US air force interpreted as a Taliban attack; and third, the admission of this kind of defence would be a real damage to the principle of sovereign equality of States; only the great powers could benefit from the detriment of the less powerful States of the diffused and inaccurate limits that exist between the preventive self-defence and the armed retaliation[787]. Gonzalez adds that admitting preventive self-defence would mean, first, to open the door to arbitrary qualification of States to legitimate the use of force in the face of an attack that still is non-existent, leading to a rise in the risk to international peace and security; and second, it is completely against the responsibility of the UNSC to control the use of force in the context of article 51[788]. Gutiérrez also emphasizes that "the doctrine of preventive war can be very dangerous"[789].

---

[783] UNGA, Doc. A/59/2005, Secretary-General's report "In larger freedom...", *op. cit.,* par. 124-125; see also TSAGOURIAS, N., "Necessity", *op. cit.*, p. 17 that mentions "any action against non-imminent threat must apply by the Security Council", see

[784] *The Chatham House principles*…, *op. cit.*, p. 971

[785] RAO, P. S., "Non-State actors and self-defence...", *op. cit.*, p. 163.

[786] CASANOVAS, O., "El principio…", *op. cit.*, 1074, PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 790; and REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 675.

[787] PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 790-791.

[788] GONZALEZ, J. D., *et al*., *Curso.., op. cit.,.* p. 1018.

[789] GUTIÉRREZ, C., "El uso de la fuerza...", *op. cit*., p. 81; see also NEUHOLD, H., *The law of international conflict..., op. cit.,* p. 141.

In this context, the IDI affirms that "The various doctrines of 'preventive' self-defence (beyond actual or manifestly imminent armed attack) do not find sufficient basis in positive International Law"[790]. Moreover, the ILA in the same direction declares that

> "If a State engages in forcible measures self-described as anticipatory self-defence but in fact not as the result of a need to prevent an imminent attack, it will not be able to avail itself of justification by self-defence and its use of force must be examined in light of the prohibitions on use of force and aggression"[791].

Thus, according to most of the doctrine, it seems that International Law does not accept preventive self-defence, only agreeing to anticipatory self-defence in case that it is necessary to face a 'manifestly imminent' threat[792].

The ICJ in the *Nicaragua case* did not pronounce about this subject since the parties only considered the right of self-defence in case of armed aggression that already occurred. Hence, the Court did not raise the issue whether a State could react against an imminent threat of an armed attack and declared that

> "In view of the circumstances in which the dispute has arisen, reliance is placed by the Parties only on the right of self-defence in the case of an armed attack which has already occurred, and the issue of the lawfulness of a response to the imminent threat of armed attack has not been raised. Accordingly the Court expresses no view on that issue"[793].

---

[790] IDI, "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*., p. 146.

[791] ILA, *Draft Report on aggression and the use of force*, *op. cit*., 2016, p. 10-11.

[792] FOCARELLI, C., "Self-defence in cyber space", in TSAGOURIAS, N.; BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2015, p. 255-283, at p. 271; ; see also O'CONNELL, M. E., "The myth of pre-emptive self-defence*", The American Society of International Law*, 2002, p. 1-21, at p. 8-11; and WAXMAN, M. C., Regulating resort to force: form and substance of the UN Charter regime, *EJIL*, 24, 2013, p. 151-189, at p. 160.

[793] ICJ, *Nicaragua case, op. cit*., par. 194.

Also, in the *Armed activities in territory of the Congo*, although Uganda asserted that a certain military operation was not constitutive of a use of force to prevent an armed attack that is anticipated it did not pronounce either[794].

Moreover, in the *Oil platforms*, although US claimed that their attacks were means to prevent new Iranian armed attacks, the Court did not take these allegations into account. Gutiérrez sets out two reasons why preventive self-defence does not reconcile with the jurisprudence established by the ICJ. First, the Court is expressed in such a way that self-defence seems only possible when *there is already* a victim of a use of armed force, not when only there is a danger or threat of such force[795]. Second, the ICJ is very classic in the treatment of the self-defence: it demands all the related requirements, with particular demands on certain occasions[796]; in addition, it insist that only the most serious uses of armed force can give rise to the right of self-defence[797]. Even some authors pointed out that the sentence offers a "restrictive" interpretation of what must be understood as armed attack[798].

Also, since the events of 11 September, the US claimed an extended right of self-defence to use military force against *rouge State* to prevent them from acquiring WMD[799]. In the same direction, another supporter of preventive self-defence, although acknowledging that the concept cannot be reconciled with International Law as it now stands, asserted that it must

---

[794] ICJ, *Armed activities in territories of Congo*, *op. cit.*, par. 118; see RIPOL, S., "La nueva doctrina …", *op. cit.*, p. 141-164.

[795] "In order to establish that it was legally justified in attacking the Iranian platforms in exercise of the right of individual self-defence, the United States has to show that attacks had been made upon it for which Iran was responsible; and that those attacks were of such a nature as to be qualified as 'armed attacks' within the meaning of that expression in article 51 of the United Nations Charter, and as understood in customary law on the use of force", see ICJ, *Oil Platforms case*, *op.cit.*, par. 51

[796] *Ibid*, par. 61 and following, par. 71 and following.

[797] *Ibid*, par. 64; and see GUTIÉRREZ, C., "El 'uso de la fuerza'...", *op. cit.*, p. 87-88.

[798] MOMTAZ, D., "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force", *Yale Journal of International Law*, 29 (2), 2004, p. 307-313, at p. 313; ORR, A. C., "Unmanned, unprecedented...", *op. cit.*, p. 736-737.

[799] US, *The National Security Strategy of the United States, op. cit.*, p. 6.

be amended in the light of ineffectiveness of NPT's non-proliferation regime and the substantial danger of *rogue States* to acquire nuclear weapons or other WMD[800].

Despite all these notable concerns, it seems these arguments are convincing, however, when the forcible counter-proliferation theory can destroy any semblance of stability in international relations and the rule of law[801].

c) *Anticipatory right of self-defence against an imminent attack*

Immediacy is a main requirement of the right of self-defence and is used in two different contexts: first, it is often seen as one of the requirements of the exercise of the self-defence alongside the necessity and proportionality; and second, in relation to an imminent or immediate threat of an act within the field of the anticipatory self-defence[802].

As is remarked *supra*, according to article 51 of the UN Charter, the right of self-defence is confined "if an armed attack occurs"; then, it is not possible against the threat of the use of force or, even, in front of the threat of an armed attack. This position is supported by the ILC that established that the threat of aggression does not allow the exercise of the self-defence[803], and by many States according their declarations in the ICJ advisory opinion on the *Legality of the nuclear weapons*[804]. Also, at the same line, the IDI *10A Resolution*

---

[800] ROBERTS, G. B. "The Counterproliferation self-help paradigm: a legal regime for enforcing the norm prohibiting the proliferation of weapons of mass destruction", *Denver Journal of International Law and Policy,* 27, 1998, p. 483-518, at p. 484; and BERES, L. R., "Israel, Iran and preemption: choosing the least unattractive option under International Law", *Dickinson Journal of International Law,* 14(2), 1996, p. 187-206, at p. 201-203.

[801] GRAHAM, Th, "National self-defense, International Law, and weapons of mass destruction." *Chicago Journal of International Law,* 4, 2003, p. 1-17, at p. 11-12; TERRY, P. C. R.; OPENSHAW, K. S., "Nuclear non-proliferation and 'preventive self-defence'; why attacking Iran would be illegal", *CYIL*, 51, 2013, p. 165-215, at p. 208-209.

[802] BELLIER, S., "Unilateral and multilateral preventives self-defense", *Maine Law Review*, 58(2), 2006, p. 508-542, at p. 514; GILL, T. D., "The temporal dimension of self-defense: anticipation, pre-emption, prevention and immediacy", in SCHMITT, M.; PEJIC, J. (eds.), *International Law and armed conflict: exploring the faultlines*, Brill, 2007, p. 113-156, at p. 115; and REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 674.

[803] ILC, "State responsibility", Documents of the thirty-second session, *Yearbook of ILC*, vol. II, part 1, 1980, p. 65-66, par. 113.

[804] ICJ, *Legality of nuclear weapons, op. cit*., Nauru, memory of 15 June 1995, p. 15; Mexico, written declaration on 19 June 1995, p. 8; or Indonesia, Doc. CR/95/25, of 3 November 1995, p. 26, among others

affirmed that "in case of the threat of the armed attack against a State, only the Security Council has the power to decide the use of force or authorize it"[805].

Nevertheless, another issue is when such threat of armed attack is imminent, given that in some circumstances the self-defence is also acceptable against an imminent attack. Thus, in some situations any further delay in countering the intended attack will result in the inability to effectively defend against the attack. In this regard "necessity will determine imminence"[806]. In this context, Israel attack to Osirak nuclear reactor of Iraq in 1981 is an appropriate example of close relation between imminent and necessity criteria when as seen *supra*, the UNSC strongly condemned the Israel attack which had failed to exhaust all peaceful means to solve the supposed threat[807].

Anticipatory self-defence refers to the use of armed force by a State to halt an imminent armed attack by another State. Hence, the State *has not yet* been victim of an attack but perceives that an act will occur in the imminent future. In fact, anticipatory self-defence is the right in the classic term of the use of force under customary International Law against an imminent threat. Under general International Law, anticipatory self-defence is inferred from *Caroline case* in 1937[808] which was later affirmed in the Nuremberg Tribunal in 1946[809].

International Law accepts that States do not need to suffer an armed attack to take lawful action to defend themselves against imminent danger of attack. In this field, legal scholars often conditioned the legitimacy of the response to an imminent threat to the visible

---

[805] IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit*, article 7.

[806] *The Chatham House principles*…, *op. cit*., p. 968.

[807] ROTHWELL, D., "Anticipatory self-defence in the age of international terrorism", *The university of Queensland Law Journal* , 24(2), 2005, p. 337-353, at p. 343-345.

[808] Noted by Mr Webster to Mr Fox on 24 April 1841 in DAMROSCH L. F., *et al., International Law..., op. cit.,* p. 923.

[809] INTERNATIONAL MILITARY TRIBUNAL (Nuremberg), judgment of 1 October 1946, reproduced in *AJIL*, 41, 1947, p. 205; and ORR, A. C., "Unmanned, unprecedented...", *op. cit*., p. 740.

mobilization of armies, navies, and air forces preparing to attack[810], such as threat was done by Iraq in the border of Kuwait in 1990.

It is unreasonable that a State waits for an actual attack to respond in the right of self-defence. At least in this field, even those who deny the right of anticipatory self-defence, may accept that once an attack has occurred, it is sufficient to trigger the right of self-defence and repel other armed attacks[811]. Also, some authors understand that the English phrase contained in article 51 *if an armed attack occurs* should not be interpreted as *only if an armed attack occurs*, since the Charter does not say this last; in other words, they recognize that there are situations in which you can admit the right of self-defence in front of an imminent attack[812]. Likewise, article 51 by emphasizing on the *inherent right* of self-defence it leaned towards preserving that the right pre-existed. While article 51 reflects the customary International Law of self-defence prior to 1945, it also recognized the ability of States to defend themselves against an imminent attack[813].

The ICJ, who made remarkable advancements towards the interpretation of the status of the use of force, only accepted "the right of self-defence in the case of an armed attack which has already occurred"[814]. Nevertheless, the Court did not pronounce about the matter of the lawfulness of the self-defence against imminent threat of armed attack[815] and seems that this issue was left open.

---

[810] See US *National Security Strategy*, 2002, *op. cit.*, p. 15; MURPHY, S. D., "The doctrine of pre-emptive…", *op. cit.,* p. 701; and WAXMAN, M. C., Regulating resort to force...", *op. cit.*, p. 160.

[811] *The Chatham House principles*…, *op. cit.*, p. 965; in this context scholars refer to the case of Afghanistan in 2001, when UK and US asserted the exercise of anticipatory self-defence in Afghanistan, see UN Doc. S/2001/946, 7 October 2001 and UN Doc. S/2001/947 of 947, 7 October 2001.

[812] See ILC, "State responsibility", *op. cit.*, vol. II, part 1, 1980, par 2, p. 65.

[813] BOWETT, D. W., *Self-defence …*, *op. cit.*, p. 187; see also NUNGESSER, D., "United States' use of the doctrine of anticipatory self-defence in Iraqi conflicts", *Pace University School of Law International Law review*, 16, 2004, p. 193-220, at p. 195.

[814] ICJ, *Nicaragua case, op. cit.*, par. 194; see also *Legality of nuclear weapons, op. cit.*, par. 38; and *Oil Platforms case, op. cit.*, par. 57.

[815] ICJ, *Nicaragua case*, *op. cit.*, par. 194; and *Armed activities on the territory of Congo, op. cit.*, par. 143; also in the *Wall* and in *Oil Platforms* case, it had opportunity to pronounce about the issue of the imminent threat of an armed attack but avoided.

In relation to anticipatory self-defence, within the framework of the UN, article 2 of the UNGA Resolution 3314 (XXIX), states that

> "The first use of armed force by a State in contravention of the Charter shall constitute *prima facie* evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity".

In fact, this provision implicitly accepts anticipatory self-defence, since it recognizes that in some cases there are long-range weapons and existing advanced techniques of detection which caused that "the first use" of the force could be noticed before an act of aggression; that is, "the traditional military signals forecasting an imminent attack often will be absent"[816]. In this case, the use of force is only justified in front of an imminent attack[817], which is not the same as notion of preventive or pre-emptive self-defence reserved to less imminent threats.

Moreover, the *High-level Panel on Security Threats* affirmed that "Threatened State according to long established International Law, can take military action as long as the threatened attack is *imminent*, no other means would deflect it and the action is proportionate"[818]. This idea is reiterated by the UNSG Report *In larger freedom* which distinguishes between *imminent threats* that "are fully covered by article 51, which safeguard the inherent right of sovereign States to defend themselves against armed attack. Lawyers have long recognized that this covers an imminent attack as well as one that has

[816] DEEKS, A. S., "Taming the doctrine...", *op. cit.,* p. 670.

[817] PÉREZ, M., "La legítima defensa...", *op. cit*., p. 200; and CASANOVAS, O., "El principio…", *op. cit*., 1074.

[818] UNGA, Doc. A/59/565, *Note [transmitting report of the High-level Panel on Threats, Challenges and Change, op. cit,* par. 188.

already happened"[819], and *latent threats* that do not justify a preventive use of armed force[820].

However, in any case, the question of whether an act of aggression is committed, is in hand of the UNSC. In this regard, the UNSC has priority to maintain international peace and security by *law enforcement measures,* except in situations when the threat is imminent and there is no time or the UNSC is unable to act[821]. Nevertheless, requirement of imminence in the context of non-State actors is not often transparent.

In contemporary International Law, in order to counter new menaces, States have attempted to adapt International Law in front of current threats. In this context, the Attorney General in the House of Lords on 21 April 2004 stated that

> "The concept of what constitutes an 'imminent' armed attack will develop to meet new circumstance and new threats […]. It must be right that States are able to act in self-defence in circumstances where there is evidence of further imminent attacks by terrorist groups, even if there is no specific evidence of where such an attack will take place or of the precise nature of the attack"[822].

Therefore, the possibility of a State to act in self-defence is confirmed where there is evidence of an imminent attack, and Brian J. Egan, Legal Advisor of the US Department of State, on 1 April 2016, in the *American Society of International Law* talking on the legal aspect of the fight of the US against the Daesh, clarifies which are the factors that the US Government has to take into account to assess if an attack is imminent. In this sense he asserts that,

---

[819] UNGA, Doc. A/59/2005, Secretary-General's report "In larger freedom...", *op. cit.*, par. 124.

[820] *Ibid,* par. 124-125; and Message of the Secretary-General to the International Conference on United Nations reform (delivered by Mr. Edward Mortimer, Director of Communications in the Office of the Secretary-General), Tehran, of 17 July 2005.

[821] SCHRIJVER, N.; VAN DEN HERIK, L., "Leiden policy recommendations...", *op. cit.*, pars. 34-37; see also SCHMITT, M. N., "Pre-emptive strategies...", *op. cit.*, p. 531.

[822] UK Attorney-General Speech in the House of Lords, HL Debates 21 April 2004, 660 c369-372; in "UK materials on International Law", *BYIL*, 75, 2004, p. 822-823.

> "When considering whether an armed attack is imminent under the *jus ad bellum* for purposes of the initial use of force against a particular non-State actor, the United States analyzes a variety of factors [...]. These factors include the nature and immediacy of the threat; the probability of an attack; whether the anticipated attack is part of a concerted pattern of continuing armed activity; the likely scale of the attack and the injury, loss, or damage likely to result therefrom in the absence of mitigating action; and the likelihood that there will be other opportunities to undertake effective action in self-defence that may be expected to cause less serious collateral injury, loss, or damage. The absence of specific evidence of where an attack will take place or of the precise nature of an attack does not preclude a conclusion that an armed attack is imminent for purposes of the exercise of the right of self-defence, provided that there is a reasonable and objective basis for concluding that an armed attack is imminent"[823].

Thus, Mr Egan left no doubt that the right of self-defence of article 51 applies to imminent threats posed by non-State actors that include terrorist groups and proposes specific criteria to assess when an imminent attack exists.

However, part of the doctrine does not accept the self-defence in front of an imminent attack and criticise that the *Secretary–General's High-Level Panel on Security Threats* as well as the UNSG itself support this interpretation. For instance, Gutiérrez affirmed that "if the armed attack does not exist, there cannot be self-defence. Therefore, this cannot be invoked before preventively in front the threat, even prior the imminence of an armed attack, since in such cases the crime remains only in the mind of the alleged guilty"[824]. Similarly, a

[823] US, EGAN, B., Legal Advisor of the US Department of State, speech on the legal aspect of the fight of the US against the Daesh, 1st April 2016, Available at https://2009-2017.state.gov/s/l/releases/remarks/255493.htm, [visited on 2 May 2018].

[824] GUTIÉRREZ, C., "El 'uso de la fuerza…", *op. cit*., p. 86; see also ANDRÉS, P., "Las normas relativas al uso de la fuerza: la seguridad colectiva y la legítima defensa en el contexto de la reforma de las Naciones Unidas", in GARCIA, C., RODRIGO, A. J., *La seguridad comprometida. Nuevos desafíos, amenazas y conflictos armados*, Tecnos, 2008, p. 113-125, at p. 114-116.

certain parallelism exists between the Reports of the *High Level Group* and the UNSG, and some passages of the US *National Security Strategy*[825].

Gutiérrez notes that the statements of the UNSG in his Report reveal "the existence of a tendency to make the concept of self-defence in particular more flexible and in general the prohibition of use of force enshrined in the Charter with its adoption"[826].

According to this new and more flexible tendency, the *Chatham House Principles* mentions that "the criterion of imminence must be interpreted so as to take into account current kinds of threat and must be applied having regard to the particular circumstances of each case"[827]. Thus, it asserts that the criteria of imminence have a close relation to the requirement of necessity. In this sense, it states that

> "Force may be used only when any further delay would result in an inability by the threatened State effectively to defend against or avert the attack against it. In assessing the imminence of the attack, reference may be made to the gravity to the attack, the capability of the attacker, and the nature of the threat, for example if the attack is likely to come without warning"[828].

Also, in this sense, the IDI mentions that

> "the right of self-defence arises for the target State in case of an actual or manifestly *imminent* armed attack. It may be exercised only when there is no lawful alternative in practice in order to forestall, stop or repel the armed

[825] "For Centuries, International Law recognized that nations need not suffer an attack before they can lawfully take action to defend themselves against forces that present an imminent danger of attack", see US, *The National Security Strategy…, op. cit.,* p. 15.

[826] GUTIÉRREZ, "El 'uso de la fuerza...", *op. cit.*, p. 99.

[827] *The Chatham House principles*…", *op. cit.*, p. 967.

[828] *Ibid.*

attack, until the Security Council takes effective measures necessary to maintain or restore international peace and security"[829].

Moreover, the *Leiden Policy Recommendation* has a little wider view. It insists on

> "whether an attack may be regarded as imminent falls to be assessed by reference to the immediacy of the attack, its nature and gravity. There must be a reasonable and objective basis for concluding that at an attack will be launched, while bearing in mind that terrorists typically rely on the unpredictability of attacks in order to spread terror among civilians. Armed force may only be used when its anticipated that delay would result in an inability by the threatened State effectively to avert the attack"[830].

Furthermore, the ILA, after recognized that "the matter remains unsettled", affirms that "there may be reason to accept that when faced with the clear and present danger of a specific imminent attack, States may engage in measures to defend themselves in order to prevent the attack"[831].

More recently, *Tallinn Manual 2.0* also admits the right of self-defence against an imminent attack asserting that "[...] a State need not wait idly as the enemy prepares to attack. Instead, a State may defend itself once the armed attack is 'imminent'"[832]. Then, according to collective legal experts in *Tallinn Manual 2.0,* resort the right of self-defence is legal against imminent threat of armed attack.

After analysing the *High-level Panel on Threats, Challenges and Change* of 2004, the *Secretary-General's report in larger freedom* and the *Chatham House Principles* of 2005, IDI 10A Resolution of 2007, *Leiden Policy Recommendation* of 2010, ILA report on aggression

---

[829] IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", *op. cit.*, article 3 (italic is ours).

[830] SCHRIJVER, N.; VAN DEN HERIK, L., *Leiden Policy Recommendations on counter-terrorism and International Law* 1 April 2010, published in *NILR,* 57(3), 2010, p. 15, p. 533-550, at p. 543, par. 46.

[831] ILA, *Draft Report on aggression and the use of force*, *op. cit.*, 2016, p. 10.

[832] *Tallinn Manual 2.0, op. cit.*, rule 73, par. 2.

and the use of force in 2016 and Tallinn Manual 2.0 rules of 2017 we can see a pattern or rather a tendency of more States towards recognizing explicitly the possibility to use the force in front imminent attacks. Thus, it seems international community generally admitted that the right of self-defence can be exercised against an imminent armed attack. However, the pre-emptive self-defence is only supported by a minority[833].

d) The right of self-defence *a posteriori*

After the events of terrorist attacks in September 2001, the US permanent representative in the UN made a declaration of intentions where it implicitly expresses that the US reserves the right to exercise the self-defence *a posterior*. In this regard, it asserted that

> "Since 11 September, my Government has obtained clear and compelling information that the Al-Qaeda organization, which is supported by the Taliban regime in Afghanistan, had a central role in the attacks. There is still much we do not know. Our inquiry is in its early stages. We may find that our self-defence requires further actions with respect to other organizations and other States"[834].

This US statement has caused misinterpretations on the right of self-defence in International Law, as it authorizes the invocation of the right of self-defence after significant time has passed since the armed attack ceased. For instance, since 2001 the US justified the use of force against Pakistan in accordance with self-defence by alleging Pakistani complicity in events of 11 September.

Although the assessment of immediacy "must be considered in the light of the time necessary to prepare the armed response"[835], *a posteriori* self-defence law goes much further. It does not claim about a current armed attack but rather about an armed attack

---

[833] For instance, US *National Security Strategy*, 2002, *op. cit*., p. 15; and BERMEJO, R., "La legítima defensa y el Derecho Internacional en los albores del siglo XXI", in *Los nuevos escenarios internacionales y europeos del derecho y seguridad*, Colección Escuela Diplomática, 7, 2003, p. 127-141.

[834] UNSC, Doc. S/2001/946, letter from the Permanent Representative of the United States of America to the President of the Security Council, 7th October 2001.

[835] REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 680.

that has already happened and is over. In fact, to admit *a posteriori* self-defence would mean to accept that any armed attack from one State against another would be able to receive an *ad infinitum* response. How can the period of time it can pass be evaluated? "The reaction cannot be described as self-defence in front of an already inexistent attack that has ceased, without forgotten that it would be difficult to inform the Security Council about the actions taken against something already completed"[836]. In *a posteriori* self-defence, actually we would be facing to an armed retaliation that is prohibited in International Law[837].

In this context, it raises the question of what kind of reaction against the attacks of September 11 would have it been according to International law. The answer seems to lie in the UNSC enforcement actions pursuant to Chapter VII of the UN Charter. If the US had reached unanimity to adopt UNSC Resolutions 1368 and 1373, among others, then it would have obtained the due authorization to activate article 42, but according to its interests the US preferred to despise the UNSC (multilateralism) and act unilaterally. That is, to provoke a loss of authority and credibility of the UN in its primary function of maintaining international peace and security[838].

Also, *a posteriori* self-defence would not fulfil the requirement of necessity. It provided that without respecting the necessary, temporal connection between attack and response, what would the need be for a victim State to protect itself?

In addition, where is the requirement of proportionality in the purposes?As Vacas points out,

> "the purpose of the use of force in self-defence cannot be other than repelling the armed attack that justified it. Once this result has been achieved, the use of force must cease, on the contrary, from that moment on, it would not be a

[836] SÁNCHEZ, L. I., *Derecho Internacional…, op. cit*., p. 194-195.

[837] RAO, P. S., "Non-State actors and self-defence...", *op. cit*., p. 170

[838] PASTOR, J. A., *Curso de Derecho…, op. cit.,* p. 791; see also MYJER, E. P. J.; WHITE, N, D., "The twin towers attack: an unlimited right to self-defence?", *JCSL*, 7(1), 2002, p. 5-17, at p. 8-10.

use of self-defence, but a new armed attack, considering that a initiative is taken on in a new episode of the use of force"[839].

Several resolutions of the UNSC have indicated the illegality of various armed actions. There it was alleged that the exercise of self-defence once after an armed attack had occurred, did not comply with the requirement of immediacy[840].

[839] VACAS, F., *El régimen.., op. cit.* p. 251.

[840] Among others, UNSC, Resolution 188, 9 April 1964; UNSC Resolution 228, 25 November 1966; UNSC, Resolution 248, 24 March 1968; UNSC, Resolution 256, 16 August 1968; UNSC, Resolution 265, 1 April 1969; UNSC, Resolution 270, 26 August 1969; UNSC, Resolution 487, 19 June 1981; UNSC, Resolution 567, 20 June 1985; and UNSC, Resolution 567, 20 June 1985.

CHAPTER III

THE RIGHT OF SELF-DEFENCE AGAINST CYBER OPERATIONS BY STATES AND NON-STATE ACTORS

Introduction

In order to find out the response of International Law to cyber operations, at first, it is necessary to ascertain the nature and scope of such operations. In other words, to determine the legal regime applicable in the context of cyber operations it is important to define and clarify the different forms of cyber operations.

The primary challenge is the terminology where the doctrine uses various terms: cyber operations[841], cyberspace operations[842], information operations[843], cyber attack[844], cyber network attack[845], computer network attack[846], cyber force[847] or cyber warfare[848]. It seems

---

[841] See ROSINI, M., *Cyber operations and the use of force in international law*, OUP, 2014, p. 10.

[842] See US *Strategic Cyberpspace Operations Guide*, Army War College, June 2016, available at https://info.publicintelligence.net/USArmy-StrategicCO.pdf, [visited on 14 January 2018; US, DoD, *Dictionary of Military and Associated Terms*, March 2018, available at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf, [visited on 23 June 2018; etc.

[843] See US *Information Operations and Cyberwar: Capabilities and Related Policy Issues,* CRS Report for Congress, September 2006, available at https://fas.org/irp/crs/RL31787.pdf, [visited on 22 May 2018; according to the *Oxford English Dictionary*, "cyber" means "relating to information technology, the internet, and virtual reality", SIMPSON, J. A.; WEINER, E. S. C., *The Oxford Compact English Dictionary,* OUP*,* 2003, p. 268.

[844] See WAXMAN, M. C., "Self-defensive force against cyber attacks: legal, strategic and political dimensions", *International Law Studies*, 89, 2013, p. 109-122.

[845] See DINSTEIN, Y., "Computer network attacks and self-defense", in SCHMITT, M. N.; O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002, p. 99-119.

[846] See ROBERTSON, H. B., "Self-defense against computer network attack under International Law", in SCHMITT, M. N.; O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002, p. 121-145.

[847] See ROSCINI, M., "World wide warfare-*jus-ad bellum* and the use of cyber force", *Max Planck UNYB*, 14, 2010, p. 85-130, at p. 96.

[848] See HOISINGTON, M., "Cyberwarfare and the use of force giving rise to the right of self-defense", *Boston College International and Comparative Law Review,* 32(2), 2009, p. 439-454; *Cyber warfare* can be defined as "*the conduct of military operations to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities'*. The key criteria that define cyber warfare are: 1) the presence of a military operation aimed at achieving a political or military advantage, 2) the causing of damage to the opponent's cyber infrastructure; and 3) the use of cyber capabilities (since computer systems can also be

more logical to use *cyber operations* instead of *cyber warfare* or *cyber attack* to avoid using outdated notions, superficial and misleading analogies[849]. However, when we are involved in a specific case of cyber attack, we will use this term. Moreover, the "terminology of war like 'cyber war' or 'cyber attack' can create situations in which a State has fewer obstacles to an aggressive response to a non-State actor's cyber threats or cyber conduct, stretching or overstepping the relevant legal boundaries"[850].

The expression *cyber attack* (which is wider than *cyber network attack*)[851] is narrower than *cyber operations;* hence, we prefer using *cyber operation* because this term covers all kinds of cyber activities that can potentially allow resorting to the use of force in self-defence.

After finding out the scope of the cyber operations, with different normative purposes, in this chapter, at first, we attempt to survey how cyber operations as use of force can violate the principle of the prohibition of threat or use of force. And second, we will see whether cyber operations constitute an armed attack to authorise the use of force in the right of self-defence. It is significant to consider that "in order for cyber operation amount to an armed attack, it has to be use of force first"[852].

---

destroyed using kinetic capabilities)", in DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*, Doc. No 77, AIV/No 22, CAVV, December 2011, p. 9, available at https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf, [visited on 25 February 2018, Cyber warfare is subset of cyber attack but this kind of cyber operation creates effects equivalent to those of conventional armed attack. Therefore, all cyber warfare has conditions of cyber attack but all cyber attacks do not have conditions of cyber warfare, see HATHAWAY, O. A., *et al*., "The law of cyber attack", *California Law Review*, 100, 2012, p. 836-837.

[849] ROSINI, M., *Cyber operations …, op. cit.,* p. 10-11.

[850] BLANK, L, R., "International Law and cyber threats from non-State actors", *International Law Studies*, 89, 2013, p. 406-437, at p. 437.

[851] ROSINI, M., *Cyber operations…, op. cit.,* p. 13.

[852] *Ibid*, p. 71.

A. **Concept, characteristics and classification of cyber operations**

1. *Definitions and characteristics of cyber operations*

Cyber attack, which falls within the broader category of cyber operation, has been broadly defined as "the use of deliberate actions, perhaps over an extended period of time to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks"[853].

There are two prominent government-led efforts to determine the scope of threat posed by cyber attacks: 1) the US Government and 2) the Shanghai Cooperation Organization (SCO)[854]. In accordance with the US Government's approach, after establishing the US Command, the Joint Chief of Staff published a lexicon in 2011 for military use in cyber operations which included the first official military definition of cyber attack. It defines cyber attack as

> "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery"[855].

---

[853] KENNETH, W. D., *et al*., quoted in DEVER, J.; DEVER. J., "Cyber warfare: attribution, preemption, and national self-defense", *Journal of Law & Cyber Warfare,* 2(1), 2013, p. 25-63, at p. 29.

[854] SCO is a security corporation group composed of China, Russia and the most of former Soviet Central Asian Republics, as well as observers including Iran, India and Pakistan; see HATHAWAY, O. A., *et. al*., "The law of cyber-attack", *op. cit.,* p. 824.

[855] US, DoD, *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories,* November 2011, available at http://www.nsci-

In accordance with the feature of this approach, cyber attacks are limited to hostile acts that are intended to harm critical cyber system. Thus, this definition restricts cyber attacks based on the *objective* of the attack[856]. In this sense, some scholars prefer a narrower definition of cyber attack and affirm that "a cyber attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose"[857]. For instance, using a computer network to operate a predator drone for kinetic attack is not a cyber attack but a technologically advanced conventional warfare. On the contrary, using a regular explosive to cut the undersea network cables which carries the information packets between continents is a cyber attack[858].

However, according to Roscini, a *cyber attack* is "a hostile use of cyber force, which could be an isolated act, the first strike of an armed conflict, an attack in the context of an already initiated armed conflict, or reaction against a previous conventional or cyber attack". This definition, which focuses on computers networks as weapons and not as objectives, does not cover kinetic attacks on computer facilities (for example, bombing a communication facility with kinetic means does not constitute a cyber attack), cyber espionage and cyber propaganda[859]. In contrast, the SCO has a rather more extensive approach to cyber attacks. According to this organization:

> "express[ed] concern about the threats posed by possible use of [new information and communication] technologies and means for the purposes [*sic*] incompatible with ensuring international security and stability in both civil and military spheres"[860].

---

va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, {visited 22 June 2018}, p. 5.

[856] HATHAWAY, O. A., *et. al*., "The law of cyber-attack", *op. cit.,* p. 824.

[857] *Ibid*, p. 826.

[858] ANTOLIN-JENKINS, V. M., "Defining the parameters of cyber war operations: looking for law in all the wrong places", *Naval Law Review,* 51, 2005, p. 132-140, at p. 138.

[859] ROSCINI, M., "World wide warfare…", *op. cit*., p. 96.

[860] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st Plenary Meeting of 2 December 2008, quoted in HATHAWAY, O. A., *et. al*., "The law of cyber-attack", *op. cit.,* p. 825.

The distinction between this interpretation and the US Government viewpoint is understandable in light of Waxman's analysis of strategic differences in the cyber attack context. As Waxman notes, "major State actors in this area are likely to have different views on legal line drawing because they perceive a different set of strategic risks and opportunities"[861].

Therefore, the SCO has accepted an expansive vision of cyber attack that includes the use of cyber technology to sabotage political stability[862]. In other words, these statements indicate that we are facing the lack of a clear definition of cyber attack and cyber operation.

The *cyber operations* fall within the broader category of *information operations* which can be defined as

> "the integrated employment of core capabilities of electronic warfare, computer network operations, psychological operations, military deceptions, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own"[863].

But, what characterizes cyber operations and makes them unique is that information can also be used to inflict disruption or damage to an adversary[864].

The US Department of Defence (DoD) defines *cyberspace operations* as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives within or

---

[861] WAXMAN, M. C., "Cyber-attacks and the use of force: back to the future of article 2(4)", *YJIL*., 36, 2011, p. 421-459, at p. 458–459.

[862] HATHAWAY, O. A., *et. al*., "The law of cyber-attack", *op. cit.,* p. 825.

[863] US, DoD, *The National Military Strategy for Cyberspace Operations*, December 2006, p. GL-2, available at file:///C:/Users/hamed/Downloads/35693%20(6).pdf, [visited on 22 March 2018; see also the updated version of US, *Joint Doctrine for Information Operation*, 2012, p. GL-3.

[864] RYAN, D. J., *et al*., "International cyber law: a normative approach", *Georgetown Journal of International Law*, 42, 2011, p. 1161-1199, at p. 1179; and ROSINI, M., *Cyber operations…, op. cit.,* p. 11; and VENTRE, D., *Information warfare,* 2nd ed., Wiley ISTE, 2016, p. 2.

through cyberspace"[865]. Also, this definition with a slightly modified language is expressed by *Tallinn Manual 2.0*[866].

The International Committee of the Red Cross (ICRC) refers to cyber operations as "operations against or via a computer or a computer system through a data stream. Such operation can aim to do different things, for instance to infiltrate a computer system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated system"[867].

The US DoD, *Assessment of International of legal Issue in Information Operation* (1999), *National Military Strategy for CyberSpace Operations* (2006), and the *Manual on International Law Applicable to Air and Missile Warfare* (2009), in their definitions of cyber operation refer to the "Computer Network Operation" (CNO). In strict linguistic terms, this notion is ambiguous and leads to mistakenly believe that only computer networks are the targets of a cyber operation, while they may also include individual and specific computers within a network as well as websites[868]. In addition, cyber operations can be carried out not only remotely through the network but also through the local installation of malware by agents that have physical access to the systems[869].

Some documents, such as the *US International Strategy for Cyberspace* (2011) and the US *DoD Strategy for Operating in Cyberspace* (2011) use *cyber space* instead of "CNO" operations; also, both the *US Presidential Policy Directive/PPD-20* (2012), and the *Tallinn Manual 2.0 on Cyber Operations* (2017), use *cyber operations* instead of "CNO"[870]. Also, Spanish *National Cyber Security Strategy* (2013), mentions that *cyberspace* is "the name given to the global and dynamic domain composed of the infrastructures of information

---

[865] US, DoD, *Dictionary of Military and Associated Terms*, March 2018, p. 60, *op. cit.*

[866] See *Tallinn Manual 2.0, op. cit.,* p. 24.

[867] ICRC, *International humanitarian law and challenges of contemporary armed conflict*, Doc. 311C/11/5.1.2, October 2011, p. 36.

[868] HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, CUP, 2013, p. 21.

[869] ROSCINI, M., *Cyber operations…, op. cit*., p. 12.

[870] US, *Joint Doctrine for Information Operation*, 2012, p. GL-3; and *Tallinn Manual 2.0.*

technology –including the Internet– networks and information and telecommunications systems"[871].

According to *Tallinn Manual 2.0* "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[872]. This definition equally applies in international and non-international armed conflict. In addition, non-violent operations, such as psychological cyber operation or cyber espionage, do not qualify as attack[873].

As a result, in this field "there are no consistent terminology or widely accepted definitions"[874]. In this sense, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) affirms that

> "There are no common definitions for cyber terms - they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements. Given this ambiguity and regardless of caveats, the glossary aims to provide a picture on how nations/States and different institutions, interpret and approach to "cyber". {...} Please note that the majority of definitions provided, are from The Tallinn Manual and strategic or policy documents such as National Strategies, therefore the information contained in this glossary does not represent a nation's position in a legal context"[875].

---

[871] SPAIN, *National Cyber Security Strategy,* 2013, Chapter I, p. 9, available at https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf, [visited on 22 May 2018].

[872] *Tallinn Manual 2.0, op. cit.,* rule 92.

[873] *Tallinn Manual 2.0…, ibid,* rule 92, par. 2.

[874] ROSCINI, M., *Cyber operations…, op. cit.,* p. 10; and DROEGE, C., "No legal vacuum in cyber space*",* 16 August 2011, available at https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, {visited on 25 April 2017}.

[875] NATO, CCDCOE, *Cyber definitions*, https://ccdcoe.org/cyber-definitions.html, {visited on 8 April 2018}.

In fact, all these matters indicate that, on one hand, there is no consistent terminology or universally accepted definitions and, on the other side, that cyber space can be at the same time the target and the mean by which an attack is delivered"[876].

Cyber operations, contrary to conventional weapons, have unique and incomparable characteristics. We can identify four features to describe cyber operations that differ from conventional attacks in the field of the use of force: indirectness, intangibility, locus factor and result[877].

The indirectness is potentially a prominent factor because several cyber operations are in need of further action by a second actor after the initial act; for instance, when the attack's target is the missile system or the disabling of systems of air traffic control[878].

The intangibility refers to a feature which neither the target of the attack nor the weapon used might exist in the real world. Its damages might be unphysical as well; for example, a cyber attack on a stock exchange. Even those attacks that have physical consequences targeting the computer data, such as the *Stuxnet* attack to Iranian atomic facilities in 2009, can be an appropriate example in this field that of attacks which modified the spinning frequencies of the centrifuges and, as a result led to physical damage to them[879].

The locus factor is related to the fact that, in some cyber operations, it may be difficult to find out of the origin of the attacks[880], because such attacks may be routed from several points in different countries in order to hide the true source; for instance, during the cyber attack

---

[876] GEISS, R.; LAHMANN, H., "Cyber warfare: applying the principle of distinction in an interconnected space", *Israel Law Review*, 45(3), 2012, p. 381-399, at p. 384; see also, ROSCINI, M., *Cyber operations…, op. cit*., p. 12.

[877] DINNISS, H. H., *Cyber warfare and the laws of war*, CUP, 2012, p. 265; and KURU, H., "Prohibition of use of force and cyber operations as 'force'", *Journal of Learning and Teaching in Digital Age,* 2(2), 2017, p. 46-53, at p. 48.

[878] DINNISS, H., *Cyber warfare…, op. cit.,* p. 265.

[879] CHIEN, E., "Stuxnet: a breakthrough, Symantec Blog", 12 November 2010, available at https://www.symantec.com/connect/blogs/stuxnet-breakthrough, {visited 22 June 2018}.

[880] SCHMITT, M. N., "Cyber operations and the *jus ad bellum* revisited", *Villanova Law Review*, 56, 2011, p. 569-605, at p. 570.

to Estonia in 2007, the malicious traffic was originated from 178 countries[881]. Hence, in the field of cyber-operations, anonymity is one of the most important characteristics[882]. In this regard, it seems that the identification and attribution of attacks provide a serious evidentiary problem. Moreover, a cyber attack can be launched without any warning[883].

The result of cyber operation "include a wide range of consequences spanning from only inconvenience to physical destruction"[884]. This infiniteness and variety of the results is "the most difficult factor in categorizing the rules on the use of force to cyber attack"[885], and such results "might, in some cases, also be more unpredictable than in the case kinetic force"[886]; for example, the cases of cyber attacks to a stock exchange or to a single bank. In addition, lapse of time between the launching of the operation and the operation and the impact is really short[887].

2. *Different classifications of cyber operations*

The different classifications of cyber operations have been known by the US documents. According to the US *National Military Strategy for Cyberspace Operations, computer network operation* (CNO) includes:

i) *Computer Network Attacks* (CNA), which are explained as "{o}perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the

[881] TIKK, E., *et al., International cyber incidents: legal considerations*, NATO CCDCE, 112, 2010, p. 23, available at https://ccdcoe.org/publications/books/legalconsiderations.pdf, {visited 2 March 2018}.

[882] BRENNER, S. W., "'At light speed': attribution and response to cyber crime/terrorism/ warfare", *Journal of Criminal Law and Criminology*, 97, 2007, p. 379-475, at p. 424.

[883] ROSCINI, M., *Cyber operations*…, *op. cit.,* p. 70.

[884] KURU, H., "Prohibition of use of force…", *op. cit.,* p. 48.

[885] *Ibid*, p. 48; and MOORE, H.; ROBERTS, D., "AP twitter hack cause panic on wall street and sends dow plunging", *The Guardian,* 23 April 2013, available at https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall, {visited on 15 February 2017}.

[886] KURU, H., "Prohibition…", *ibid*; and SCHMITT, M. N., "Computer network attack and the use of force in International Law: thoughts on a normative framework", *Columbia Journal of Transnational Law*, 37, 1999, p. 885-926, p. 891.

[887] ROSCINI, M., *Cyber operations*…, *op. cit.,* p. 70.

computers and networks themselves"[888]. A more accurately definition of CNA is "actions {...} taken *through the use of computer networks* to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves"[889]. Hence, the concept of CNA is *narrower* than *cyber attack,* which can operate not only through computer networks, but also through close access to systems with evil intentions[890]; for example, attacks on computer systems which are intended to degrade or destroy the infrastructure capability.

ii) *Computer Network Defence* (CND) is defined as "{a}ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks"[891]. In this sense, CND employs information assurance, capabilities, intelligence, counterintelligence, law enforcement, military capabilities, which include both active cyber defences ("launching a pre-emptive, preventive, or cyber counter-operation against the source")[892] and passive cyber defences (measures "for detecting and mitigating cyber intrusions and the effects of cyber attacks that does not involve launching a preventive, pre-emptive or countering operation against the source"; for instance, firewalls, patches, honeypots, anti-virus software and digital forensics tools)[893].

iii) *Computer Network Exploitation* (CNE) are conceptualized as "{e}nabling operations and intelligence collection to gather data from target or adversary automated information systems or networks"[894], which must occur "through the use of computer networks"[895]. Also, more ambiguously, NATO defines CNE as "{a}ction taken to make use of a computer or

---

[888] US *The National Military Strategy for Cyberspace Operations*, 2006, p. GL-1; a very similar definition appears in NATO's *Glossary of Terms and Definitions*, AAP-06, Edition 2017, p. 27, available at file:///C:/Users/hamed/Downloads/AAP-06%202017%20(1).pdf, [visited on 22 June 2018].

[889] US *Joint Terminology for Cyberspace Operation,* 2010, p. 3 (italic is ours), available at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, [visited on 6 March 2018].

[890] ROSCINI, M., *Cyber operations*…, p. 13.

[891] US, DoD, *The National Military Strategy for Cyberspace Operations*, December 2006, p. GL-1, *op. cit.*

[892] *Tallinn manual, op. cit,* p. 257.

[893] *Tallinn manual, op. cit,* p. 261.

[894] US, DoD, *National Military Strategy for Cyberspace Operations*, 2006, p. GL-1, *op. cit.*

[895] US *Joint Terminology for Cyberspace Operation,* 2010, p. 4, *op. cit.*

computer network, as well as the information hosted therein, in order to gain advantage"[896]. NATO's *Glossary of Terms in Definitions* only distinguishes between CNA and CNA and does not include CND.

The US *DoD Dictionary of Military and Associated Terms* uses an alternative classification which distinguished *cyberspace operations* according to their purpose in *Defensive Cyberspace Operation* (DCO) for instance, "{p}assive and active cyber space operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated system", and *Offensive Cyberspace Operations* (OCO), which are those "intended to project power by the application of force in or through cyberspace"[897].

Finally, the US *Presidential Policy Directive/PPD-20* classifies c*yber operations* in: i) *Cyber Collection* (CC) which mainly corresponds to CNE, are

> "{…} operations and related programs or activities conducted by or on behalf of the United State government, in or through cyberspace, for the primary purpose of collecting intelligence -including information that can be used for future operations- from computers, information or communications systems, or networks with the intent to remain undetected"[898];

and ii) *Cyber Effects Operations* (CEO) whose aim is to achieve a "cyber effect", defined as the "manipulation, disruption, denial, degradation, or destruction of computers, information or communication systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon"[899].

In fact, what all these classifications have in common is the main distinction between cyber exploration and cyber attack. As we have seen *supra*, the "primary technical difference

---

[896] NATO's *Glossary of Terms and Definitions*, AAO-06, 2014, p. 2-C-11.

[897] US, DoD, *Dictionary of Military and Associated…, Terms,* March 2018, p. 65 and 170.

[898] US, *Presidential Policy Directive/PPD-20*, of October 2012, p. 2, available at https://fas.org/irp/offdocs/ppd/ppd-20.pdf, [visited on 22 June 2018].

[899] *Ibid*.

between cyber attack and cyber exploitation is in the nature of the payload to be executed- a cyber attack payload is destructive whereas a cyber exploitation payload acquires information non-destructively"[900]. Although they are often named in the mass media as *cyber attacks*, cyber exploitation operations "are different which as they do not affect the system's operation"[901]. They focus more on the intelligence collection and observation than on the network disruption and can be preliminary to an attack[902].

B. **Cyber operations as violation of the principle of the prohibition of the threat or use of force**

In this part, firstly, we are going to examine the cyber operations that can constitute violation of the principle of the prohibition of the use of force and those operations that can breach the prohibition of the threat of force. Finally, we will analyse the cyber operations that may be considered below the level of the use of force.

1. *Cyber operations and other related activities as use of force*

Cyber operations are classified into three categories: first, those operations and other related activities that are equivalent to the threat or use of force; second, those cyber operations below the level of use of force; and third, those cyber operations that amount to an armed attack in the sense of authorizing the exercise of the right of self-defence. In this section, we are going to analyse the first two categories.

a) *Cyber operations as use of force*

Because of the lack of a precise clarification of what kind of actions violate the principle of the prohibition of the use of force in International Law, during the last decades States and non-State actors had motivation to conduct a wide range of cyber operations among each other for different purposes. Thus, such operations raise the question of whether cyber

[900] LIN, H. S., "Offensive cyber operations and the use of force", *Journal of National Security Law and Policy,* 4, 2010, p. 63-86, at p. 64.

[901] See ROSCINI, M., *Cyber operations…, op. cit*., p. 16.

[902] WATTS, S., "Combatant status and computer network attack", *VJIL,* 50(2), 2010, p. 391-447, at p. 392-400.

operations can violate the principle of the prohibition of the use of force in International Law.

The key *ius ad bellum* and *ius in bello* instruments in International Law are The Hague Conventions of 1899 and 1907, the UN Charter of 1945, and the four Geneva Conventions on the protection of victims of war of 1949 and their two Additional Protocols of 1977, but none of them refer to the cyber issue. In the context of criminal cooperation, at the universal level, for instance, Resolution 45/121, adopted by the UNGA, calls upon States to cooperate with each other during the investigation and prosecution of international crimes[903] and, at the European regional level we find the Convention on Cybercrime[904].

In fact, these changes in the security environment and the emergence of new threats in cyber space caused the concern of OSCE PA, underlining that "cyber attacks have become a serious security threat, which cannot be underestimated" [905], and affirming that "the result of a cyber attack against vital State infrastructure do not differ in nature from those of a conventional aggressive act[906]".

In this regard, the ICJ in the Advisory Opinion on *South West Africa,* declared that "an international instrument has to be interpreted and applied within the framework of the

[903] Resolution 45/121 on the prevention of crime and the treatment of offenders, 14 December 1990; see also; UNGA, Resolution 40/32 on the prevention of crime and the treatment of offenders, 29 November 1985; UNGA, Resolution 42/52 on "Efforts and measures for securing the implementation by States and the enjoyment by youth of human rights in conditions of peace, particularly the right to education and to work", 30 November 1987; and UNGA, Resolutions 44/72 on "Crime prevention and criminal justice", 8 December 1989.

[904] COUNCIL OF EUROPE, Convention on Cybercrime, 23 November 2001; it was elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and U.S, and entered into force on 1 July 2004; has been ratified by 26 States (France, Germany, Italy, U.S…) and signed by 20 States (Japan, U.K, Spain...).

[905] OSCE PA, "Resolution on Cyber Security and Cyber Crime", *Astana Declaration of the OSCE Parliamentary Assembly and Resolutions adopted at the Seventeenth Annual Session*, 3 July 2008, par. 3.

[906] OSCE PA, "Resolution on Cyber Security and Cyber Crime", *Astana Declaration…, ibid,* par. 19; identically reiterated in "Resolution on Cyber Crime", OSLO, *Declaration of the OSCE Parliamentary Assembly and Resolutions adopted at the Nineteenth Annual Session*, 10 July 2010, par. 7; and in similar terms repeated in "Enhancing Mutual Trust and Cooperation for Peace and Prosperity in the OSCE Region", *Minsk Declaration and Resolutions adopted by the OSCE Parliamentary Assembly at the Twenty-sixth Annual Session*, 9 July 2017, par. 76.

entire legal system prevailing at the time of the interpretation"[907]. Also, dynamic interpretation is implied in article 3(b) of 1969 Vienna Convention on the Law of Treaties.

In this sense, the US *International Strategy for Cyberspace* of 2011 asserts that "The development of norms for State conduct in cyberspace does not require a reinvention of customary International Law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace"[908]. Also, *Tallinn Manual* confirms that "both the *ius ad bellum* and *ius in bello* apply to cyber operations"[909]. Thus, the existing rules and principles of International Law are applicable to cyber space[910].

Article 2(4) of the UN Charter is the key prescription in International Law which describes unlawful uses of force; on one hand, as acts against the *territorial integrity* and *political independence* of the State and, on the other hand, as acts that *are inconsistent with the purposes of the UN.* Thus, the last phrase implies that such acts, despite not even directed against the territorial integrity or political independence of a State, may violate the rule of the prohibition of the use of force if they are inconsistent with the purposes of the UN Charter. Nowadays, it is widely accepted that the principle of the prohibition of the use of force applies to any use of force which is not permitted by any term of the UN Charter[911].

---

[907] ICJ, *Legal Consequences for States of the continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* advisory opinion, 21 June 1971, *ICJ Reports 1971,* par, 53.

[908] US, *International strategy for cyberspace. Prosperity, security, and openness in a networked world,* the White House, May 2011, p. 9, available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, [visited on 11 June 2018].

[909] *Tallinn Manual, op. cit.*, p. 19.

[910] See the answer of Koh, Legal Advisor of the US Department of State, to the question "Do established principles of International Law apply to cyber space? Yes, International Law principles do apply in cyberspace", KOH, H. H., "International Law in cyberspace", *HILJ Online*, 54, 2012, p. 2-3, available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers, {visited on 22 June 2018}; and EGEDE, E.; STUTCH, P., *Politics of International Law..., op. cit.,* p. 262-263.

[911] ILA, *Draft Report on aggression and the use of force, op. cit.*, 2016, p. 2-3.

There is not an official definition of what constitutes the use of force in International Law, but some parameters are well-defined[912]; as mentioned in the Second Chapter, traditionally the term use of force is limited to the armed force by a State. Therefore, the armed force includes kinetic force, dropping bombs or firing artillery[913]. Despite the attempts made by developing States to include economic and political coercion into article 2(4) during the drafting of the UN Charter and UNGA resolutions, ultimately both the economic and political coercions remained outside the scope of article 2(4) and are currently described in the scope of the principle of non-intervention.

In this context, although historically the US was in favour of restricting the standards for understanding article 2(4), nowadays, as a result of networked information infrastructures and global economic linkages, it certainly "has an interest in expanding the Charter, at least at the edges, so as to cover some hostile cyber-activities that might not fit within its traditional understanding of 'force' or the triggers of self-defence rights"[914]. In this sense, the former US Legal Advisor Koh declared that if the effects of the action by kinetics constitute the use of force, then cyber operations with the same effects can constitute the use of force[915].

According to the *interpretive reorientation approach*[916], the idea "that cyber attacks *could* constitute force or armed attack is not inconsistent with the narrow interpretations generally advocated by the United State during most of the Charter's history"[917]. In this direction, Roscini mentions that

---

[912] BARKHAM, J., "Information warfare and International Law on the use of force", *New York University Journal of International Law and Politics,* 34, 2001, p. 57-97, at p. 70.

[913] SCHMITT, M. N., "Cyber operations…", *op. cit*., p. 154.

[914] WAXMAN, M. C., "Cyber-attack and…", *op. cit*., p. 437; and BROWNLIE, I., *International law…, op. cit.,* p. 362.

[915] KOH, H. H., "International Law in cyberspace", *HILJ Online*, 54, 2012, p. 3-4, available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers, {visited on 22 June 2018}.

[916] WAXMAN, M., "Cyber-attack and use of force…", *op. cit*, p. 437.

[917] *Ibid*.

> "existing *jus ad bellum* and *jus in bello* provisions to adapt cyber technology are supported by many States when they affirmed the application of current laws comprising the UN Charter and law of armed conflict to cyber operation without distinguish between treaties and customary norms"[918].

The potential application of article 2(4) to cyber operation creates interpretative difficulties on the distinction between force and coercion. In other words, in order to include all cyber operations in the scope of the principle of the threat or use of force, a major extensive definition of article 2(4) is needed, because it seems that traditionally International Law is excluded them from such article, and by them I mean all those cyber attacks that do not cause physical damage, such as electronic incursions and blockades which are equivalent to acts of economic and political coercion[919].

Ultimately, in this context, to determine whether a cyber operation can violate the principle of the prohibition of the use of force, three analytical approaches are accepted: *instrument-based approach, target-based approach and the effect-based approach*[920]. The *instrument-based approach is* simply focused on the use of military weapons. This approach was dominant during the Cold War in its pre-cyber years[921]. After the Cold War, there were serious discussions where some scholars emphasized that article 2(4) does not explicitly refer to arms[922] and non-military weapons. Although they provoke serious physical damages they can never constitute a use of force under article 2(4) [923].

---

[918] ROSCINI, M., *Cyber operations*…, *op. cit*., p. 21.

[919] BARKHAM, J., "Information warfare…", *op. cit*., p. 84-85.

[920] ROSCINI, M., *Cyber operations*…, *op. cit*., p. 46.

[921] DECOULARE-DELAFONTAINE, N., "Cyber attacks on nuclear facilities and nuclear responses to cyber attacks in International Law", December 17, 2015, p. 1-35, at p. 5, available at http://lcnp.org/pubs/studentpapers/2016/Cyber%20Attacks%20-%20Nina.pdf, {visited on 22 June 2018}.

[922] Article 2(4) is not limited only to requirement of kinetic force when effects of non kinetic may be worse and give rise to "destruction to life and property", *cfr*. BROWNLIE, I*., International law…, op. cit.,* p. 362; also Dinstein assert "{i}t doesn't matter what specific means-kinetic or electric-are used to bring it about, but the end result must be that violence occurs or is threatened", DINSTEIN, Y., *War, aggression…, op. cit.,* p. 89-90.

[923] *Cfr*., among others, WAXMAN, M. C., "Self-defensive…", *op. cit.,* p. 111; and HANDLER, S. G., "New cyber face of battle: developing a legal approach to accommodate emerging trends in warfare", *Stanford Journal of International* Law, 48, 2012, p. 209-238, at p. 226-227.

Moreover, some doctrine emphasized on broader interpretations extending the legal prohibition "to all coercion, by whatever instrument or combination of instruments, military and other, which is directed with requisite against such substantial bass of power as the 'territorial integrity' and 'political independence' of the target State"[924].

Likewise, the *instrument-based approach*, is denied by the US Statement in 1999, when the US Defence Department's Office of the General Counsel produced an *Assessment of International Legal Issues in Information Operations* that reported:

> "If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack that its mechanism"[925].

Also, such approach was rejected by the ICJ in 1996 which pointed out that article 2(4) "do{es} not refer to specific weapons {but} appl{ies} to any use of force, regardless of the weapons applied. The Charter neither expressly prohibits, not permits, the use of any specific weapon, including nuclear weapons"[926]. Therefore, the *instrument-based* approach is over timed and difficult to be applicable in cyber space operations[927].

The *target-based approach* is an extension of the use of force to lower levels of the use of force; it means that it increases the risk of responding even to minor attacks[928]. This approach argues that cyber operations against a National Critical Infrastructure (NCI)

---

[924] MACDOUGAL, M. S.; FELICIANO, F. P., *The International Law of war: transnational coercion and world public order*, Martinus Nijhoff, 1994, p. 259; see also REISMAN, W. M., "Coercion and self-determination: construing Charter article 2(4), *AJIL*, 78(3), 1984, p. 642-645, at. p. 642 and 644.

[925] US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment of International Legal Issue in Information Operations* , Washington, May 1999, p. 18, available at http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, [visited on 2 March 2018].

[926] ICJ, *Legality of the threat or use of nuclear weapons,* advisory opinion, 8 July 1996, *ICJ Reports 1996*, par. 39.

[927] HATHAWAY, O. A., *et al*., "The law of cyber-attac", *op. cit.,* p. 846.

[928] KURU, H., "Prohibition of use of force…", *op. cit.,* p. 45-47.

violate article 2(4) of UN Charter[929]. This point of view is over inclusive and the prohibition of the use of force also covers those operations that only cause inconvenience or merely aim to collect information whenever they target a NCI[930]. In fact, they assert that stealing or compromising data that is considered vital for the national security, such as sensitive military information, and can be qualified as an armed attack "even though no immediate loss of life or destruction results"[931].

On the other hand, the *effect-based approach* (equivalence-based or result-oriented approach) is under the support of most of the legal scholars[932]. In this sense, Clarke and Knake propose the Obama doctrine of "cyber equivalency, in which cyber attacks are to be judged by their effects not their means. They would be judged as if they were kinetic attacks and may be responded to by kinetic attacks or other means"[933].

Moreover, some doctrine believes that there is no difference between an attack by firing a missile to a target and cyber attacks that can cause physical damage[934]. For instance, following Brownlie's approach, if cyber attacks have the same result as bombs or bullets, as

---

[929] SHARP, W. G., *Cyberspace and the use of force*, Aegis Research Corporation, 1999, p. 129-132.

[930] ROSCINI, M., *Cyber operations…, op. cit*., p. 47.

[931] JOYNER, C. C.; LOTRIONTE, C., "Information warfare as international coercion: elements of a legal framework, *EJIL*, 12(5), 2001, p. 825-865, at p. 855.

[932] BUCHAN, R., "Cyber attacks: unlawful uses of force or prohibited interventions?", *Journal of Conflict and Security Law,* 17(2), 2012, p. 211-227, at p. 212; DINNISS, H., *Cyber warfare… ,op. cit.,* p. 74; and SCHMITT, M. N., *Cyber operations…", op. cit*., p. 155-156; see also *Tallinn Manual 2.0, op. cit,* rule 69, par. 1; and CARR, J., *Inside cyber warfare: mapping the cyber underworld*, O'Reilly Media, 2011, p. 59.

[933] CLARKE, R. A.; KNAKE, R. K., *Cyber war. The next threat to national security and what to do about it*, Harper Collins e-books, 2014, p. 87, available at http://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf, [visited on 8 June 2018]; see Barack Obama addressing the graduating class of one of the four US military academies (Obama Doctrine): "So let me make this clear to any nation that may contemplate using cyber weapons against us. The United States will regard a cyber attack that disrupts or damages our military, our government, or our critical infrastructure as we would a kinetic attack that had the same target and the same effect. We would consider it a hostile act in our territory. In response to such aggression in our cyberspace, I, as Commander in Chief, will draw upon the full panoply of power available to the United States of America and will not be limited as to the size or nature of our response by those characteristics of the attack upon us", p. 86.

[934] BROWN, D., "A proposal for an international convention to regulate the use of information systems in armed conflict", *HILJ,* 47, 2006, p. 179-221, at p. 187.

a result, they can fall under the prohibition of the use of force[935]. Thus, under the *effect-based* approach, many States and scholars agree that cyber attacks can constitute a violation of the principle of the prohibition of the use of force[936].

Furthermore, the *effect-based* approach is adopted by the US *National Research Council*. In this regard, cyber attacks should be judged under the UN Charter and customary *ius ad bellum* principles by considering the effects of cyber attacks when they have a clear resemblance to a military attack[937]. Likewise, such Council asserted the "death or personal injury to people and destruction of physical property as criteria for the definition of the use of force"[938]. In this sense, the fact that the US Government supports the effect-based approach does not mean that some activities, such as the computer–based espionage and intelligence collection constitute a use of force because these activities do not produce direct or indirect destructive consequences parallel to a military attack[939].

Moreover, *Tallinn Manual 2.0* developed a range of assessment factors to determine whether cyber acts constitute use of force. In this sense, this group of legal experts, under the influence of the ICJ judgment in *Nicaragua case,* proclaim that cyber operations can constitute a use of force when its scale and effects are comparable to a non-cyber operations rising to the level of a use of force. Therefore, all cyber operations with analogous scale and effects to other kinetic or non-kinetic actions are considered uses of

---

[935] See BROWNLIE, I., *International law*..., *op. cit*., p. 362-363.

[936] Among others SILVER, D. B., "Computer network attack as a use of force under article 2(4) of the United Nations Charter", in SCHMITT, M. N.; O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002, p. 74-97, at p. 81-82; REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 690; and WAXMAN, M. C., "Cyber attacks as 'force' under UN Charter article 2 (4)", *International Law Studies,* 87(1), 2011, p. 43-57, at p. 52-53; DUCHEINE, P.; *et al*. (eds.), "Towards a legal framework for military cyber operations", ARMS Netherlands Annual Review of Military Studies, 2012, p. 101-128, at p. 116; REMUS, T., "Cyber-attacks and International Law of armed conflicts; a *jus ad bellum* perspective", *Journal of International Commercial Law and Technology*, 8(3), 2013, p. 179- 189, p. 181; and EGEDE, E.; STUTCH, P., *Politics of International Law..., op. cit.,* p. 262-263.

[937] US, NATIONAL RESEARCH COUNCIL, *Technology, policy, law, and ethics regarding US acquisition and use of cyber attack capabilities*, National Academies Press, 2009, p. 33-34.

[938] *Ibid*., p. 253.

[939] *Ibid*., p. 259-261.

force[940]. In fact, the common sense tells us that, if consequences of cyber operations are equated with physical damage of dropping a bomb or firing a missile, they should also be considered a use of force[941]. In this context, some supporters of the *effect-based* approach assert that "whether an attack is to be considered as an armed attack depends on the consequence of the attack rather than the modalities"[942].

Both the level of harm inflicted, and certain qualitative aspects of a cyber-operation are useful elements to indicate some informal legal criteria to identify cyber operations as use of force. In the framework of the *effect-based* approach, following the *Tallinn Manual 2.0*, the factors to assess whether a cyber operation constitute a use of force are severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement and presumptive legality[943].

i) *Severity* is the key factor to constitute the use of force by cyber operations. According to this factor, acts with physical harm to individual or property are qualified as use of force, especially acts that effect on the critical national interests. However, those acts generating mere irritation or inconvenience will never constitute use of force. Hence, scope, duration and intensity of circumstances are very important on the appraisal of their severity. As a result, damage, destruction, injury or death by cyber operations would probably constitute a use of force.

ii) *Immediacy*: according to the character of cyber operation, those that produce immediate effect or results are more likely to use force rather than other which are delayed and take weeks or months to achieve their intended effects.

iii) *Directness*: the cause and effect of cyber operations must be clearly linked to the characterization of the use of force. Whereas the immediacy factor focuses on the temporal

---

[940] The ICJ alleged that *scale* and *effect* are useful criteria to identifies acts qualify as use of force, in particular, armed attack under article 51, see ICJ, *Nicaragua case, op. cit*., par. 195; and *Tallinn Manual 2.0, op. cit.,* rule 69, par. 9.

[941] KOH, H. H., "International law…", *op. cit*., p. 4.

[942] ROBERTSON, H, B., "Self-defense against…", *op. cit*., p. 133.

[943] See *Tallinn Manual 2.0, op. cit.,* rule 69, par. 9.

aspect of the consequences, directness examines the chain of causation. Cyber operations whose causes and effects are clearly linked are more likely to be characterized as uses of force.

iv) *Invasiveness* refers to the degree to which cyber operations penetrate into the cyber system of the target State or its interests. As a rule, the more secure a targeted cyber system is, the greater the concern as to its penetration. Also, the degree to which the intended effects of a cyber operation are limited to a particular State increases the perceived invasiveness of those operations. Domain name is a highly visible indicator in cyberspace and may be highly significant when assessing the extent of invasiveness of an operation. Therefore, those cyber operations that target the domain name of the State or its particular organs, can be more invasive than those cyber operations directed at non-State specific domain name extension such as 'come'. In this regard, even the most highly invasive cyber espionages do not rise to the level of the use of force due to the absence of a direct prohibition in International Law on espionage *per se*.

v) *Measurability of effect* is a factor that refers to actions as a use of force when the consequences are apparent. Contrary to the traditional armed force operations whose effects are usually measurable, consequences of cyber operations are less apparent. Thus, a cyber operation that can be evaluated in very specific terms (for instance, the amount of data corrupted, percentage of servers disabled, or number of confidential files infiltrated, is more likely to be characterized as a use of force than one with difficulties when measuring it or with subjective consequences).

vi) *Military character*: traditionally, the use of force has been employed by military or other armed forces. In this sense, the connection between cyber and military operations is the characterization of the use of force.

vii) *State involvement*: the amount of involvement of a State in cyber operation lies along a continuum from operations conducted by a State itself. For example, activities of its armed force or intelligence agencies to those whose involvement is peripheral. The clearer and

closer a nexus between a State and cyber operations are, the more likely it is that other States will characterize them as uses of force by that State.

viii) *Presumptive legality*: according to International Law, acts that are not forbidden are permitted. Thus, acts like propaganda, psychological operations, espionage or economic pressure *per se*, are presumptively legal. This being so, they are less likely to be considered by States as uses of force.

As mentioned in the *Tallinn Manual 2.0,* on one hand, these factors are not exhaustive and "depending on the attendant circumstances, State may look to others, such as prevailing political environment, whether cyber operation portends the future use of military force, the identity of attacker, any records of cyber operations by the attacker, and the nature of the target (such as critical infrastructure)" and, on the other hand, "the factors operate in concert"[944].

According to Roscini, cyber operations produce three effects: *primary effects* are on the attacked computer, computer system or network, such as deletion, corruption, alteration of data, software or system disruption through a Distributed Denial-of-Service (DDoS) attack or other cyber attack; *secondary effects* are on infrastructures operated by the attacked system or network, for instance, its partial or total destruction or incapacitation; and *tertiary effect* which are on the persons affected by such destruction or incapacitation of the attacked system or infrastructure. Hence, secondary effects are limited to damages to physical property and tertiary effects on death and injury of persons[945].

There are two important practical cases that can help to better understand what sort of cyber operations can constitute a use of force: Estonia in 2007 and Iran in 2010. In Estonia, large botnets applied against government agencies and private companies, such as media stations and banks. Essentially, these cyber attacks were a kind of DDoS where Internet websites were disrupted and ran extremely slowly or even crashed completely. The Foreign and Justice ministries and the two largest banks crippled. These attacks lasted

[944] *Tallinn Manual 2.0,* rule 69, par. 10.

[945] ROSCINI, M., *Cyber operations*…, *op. cit*., p. 52-53.

approximately three weeks, from 26 April to 19 May. Even though Estonia's Government accused Russia of these cyber attacks, the Russian Government denied responsibility and no definite attribution has ever been made. Ergma, speaker of the Estonian Parliament asserted that "when I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing {…} like nuclear radiation, cyber war does not make you bleed, but it can destroy everything"[946].

Although these attacks caused damage, it did not give rise to any physical damage. In other words, no lives were lost, no troops crossed the border and no gun was fired. Hence, given the absence of physical damages or critical infrastructure disruption, it did not constitute a use of force[947]. In this sense, *Tallinn Manual 2.0* states that "A highly invasive operation that causes only inconvenience, such as temporary denial of services, is unlikely to be classified as use of force. By contrast, some may categorise massive cyber operations that cripple an economy as a use of force, even though economic coercion is presumptively lawful"[948].

In Iran, in July 2010 the Natanz Nuclear Plant suffered from Stuxnet attacks virus. Natanz is a nuclear plant that was used to enrich uranium. To achieve that, it was placed in centrifuges under a specific speed, temperature and pressure. The Stuxnet virus was designed to change the rotor speed of centrifuges by increasing and decreasing its speed, and, as a result, the system was producing uranium below the optimal level. This virus operated covertly, and the operation of centrifuges seemed normal and the presence of virus was not visible[949]. The cyber attack on nuclear facilities did not make any explicit impact, but if Stuxnet disrupted the correct speed of centrifuges and prevented an optimal enrichment of uranium we can claim that the cyber attack damaged the physical property. According to *reports* of Institute for Science and International Security[950] and Iranian

---

[946] ERGMA, E., quoted in BUCHAN, R., "Cyber attacks…", *op. cit*., p. 218.

[947] BUCHAN, R., "Cyber attacks…", *ibid*, p. 219; see also HINKLE, K. C., "Countermeasures in the cyber context: one more thing to worry about", *YJIL*, 37, 2011, p. 11-21, at p. 13.

[948] *Tallinn Manual 2.0, op. cit.,* rule 69, par. 10.

[949] SHAKARIAN, P., *Stuxnet: cyberwar revolution in military affairs*, Military Academy West Point, 2011, p. 1-3.

[950] The Institute asserted that vibrations could be sufficient to destroy the centrifuges, therefore *Stuxnet* virus was a reasonable explanation for the damage at Natanz; see ALBRIGHT, D., *et al*., *Did Stuxnet take out 1.000 centrifuges at the Natanz enrichment plant?*, Institute for Science and International Security, 22 December

officials, physical destruction on centrifuges occurred and, therefore, the violation of the principle of the prohibition of the use of force was possible[951].

It seems that it is widely accepted that "cyber attack that cause or reasonably likely to cause physical damage to property, loss of life or injury to persons would fall under the prohibition contained in article 2(4) of the UN Charter"[952]. Although this article is generally applied to armed forces, if the international community followed Brownlie's view that biological and chemical weapons are a form of force because they can "destroy life and property"[953], by the same logic, a computer attack that can destroy property or injury people can constitute use of force[954].

In this regard, cyber operations with grave destructive consequences can violate the principle of the prohibition of the use of force. Therefore, there is consensus in "acts that injure or kill persons or physically damage or destroy objects are uses of force ({...} but requiring the harm to be 'significant')"[955]. In this sense, NATO declared that its defence commitments might extend to collective response to cyber space[956]. Nevertheless, cyber operations that just caused damages, such as the destruction of a single computer or server, cannot constitute the use of force[957]. In any case, there is serious controversy on whether the destruction or damage of data without any physical damage or incapacitation of infrastructure can violate the principle of the prohibition of the use of force.

2010, available at http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf, {visited on august 2017}.

951 BUCHAN, R., "Cyber attacks…", *op. cit.*, p. 220-221; and MURPHY, J. F., "Cyber war and International Law: does the International Law process constitute a threat to U.S vital interests?", *International Law Studies*, 89(1), 2013, p. 309-340, at p. 315.

952 ROSCINI, M., *Cyber operations…*, *op. cit.*, p. 53; see also HOISINGTON, M., "Cyberwarfare…", *op. cit.*, p. 447; and SCHMITT, M. N., "Computer network attack and the use of force in International Law: thoughts on a normative framework", *Columbia Journal of Transnational Law*, 37, 1999, p. 913.

953 BROWNLIE, I., *International law…, op. cit.*, p. 362.

954 JOYNER, C. C.; LOTRIONTE, C., "Information warfare...", *op. cit.*, p. 849.

955 *Tallinn Manual 2.0, op. cit.,* rule 69, par. 8; also Koh asserts that "cyber activities that proximately result on death, injury or significant destruction" can constitute use of force, KOH, H. H., "International law…", *op. cit.*, p. 4.

956 NATO, "Cyber defense", available at https://www.nato.int/cps/en/natohq/topics_78170.htm {visited on 10 November 2017}.

957 ROSCINI, M., *Cyber operations…*, *op. cit.*, p. 54.

Nowadays, in a modern society where "heavy reliance on interconnected information systems means that the indirect and secondary effects of cyber attacks may be much more consequential than the direct and immediate one"[958], it seems that the nature of data, particularly that which is considered vital to national security, is very important to determine the existence of the use of force. In this regard, if a foreign government attacks the computer databases of another State's departments or ministry of defence and steals classified information about to nuclear weapons' launch instruments," such actions could qualify as being tantamount to 'armed attacks', even though no immediate loss of life or destruction results"[959].

b) *Potential activities related to cyber operations that can constitute an indirect use of force*

As we have seen, in conformity with the ICJ's view in the *Nicaragua case*, not only does the direct use of force by one State against another State fall under the principle of the prohibition of the use of force, but also the indirect uses of force, such as the arming and training of non-State actors, can violate such principle[960]. Hence, organizing a group with malware and teaching it to use it to carry out cyber attacks against another State, would be qualified as use of force[961]. However, the support to non-State actors to conduct cyber operations that are below the threshold of the use of force cannot violate the principle of the prohibition of the use of force.

Under the context of article 3(f) of the UNGA Resolution 3314 (XXIX) on the definition of aggression, if a State knowingly authorizes another State to use its infrastructures to launch a cyber attack it amounts to an act of aggression and would violate the principle of the

[958] WAXMAN, M. C., "Cyber attacks and the use of force…", *op. cit*., p. 445.

[959] JOYNER, C. C.; LOTRIONTE, C., "Information warfare...", *op. cit*., p. 855.

[960] "In the view of the Court, while the arming and training of the *contras* can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government", ICJ, *Nicaragua case, op. cit*., par. 228.

[961] *Tallinn Manual 2.0…, op. cit.,* rule 69, par. 4.

prohibition of the use of force[962]. In fact, the supply of a sanctuary along with other acts, such as the substantial support or provision of cyber defences to non-State actors, in certain circumstances, can constitute use of force[963]. However, in most of the cases, simply granting sanctuary is insufficient to attribute the action of a non-State actors to the host State to justify the use of force in the right of self-defence by the victim State.

Also, this view is affirmed in article 8 of the ILC Draft on State responsibility where it states that "the conduct of a person or group of persons shall be considered an act of a State under International Law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, the State in carrying out the conduct"[964]. In this regard, there must be a real link between the person or group performing the act and the State[965].

2. *Cyber operation as threat of force*

As mentioned *supra*, threat of force in International Law can be defined explicitly and implicitly through statements or actions to the future unlawful use of force; the existing threat depends on the hostile intention of the threatener. In the context of cyber operations, *Tallinn Manual 2.0* asserts that "a cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force"[966]. However, cyber threats exercised under the right of self-defence are not unlawful. Thus, "threatening destructive defensive cyber attacks against another State military infrastructure if that State unlawfully mounts unlawful cross border operation would not breach the norms"[967].

---

[962] ROSCINI, M., *Cyber operations…, op. cit*., p. 67.

[963] *Ibid*, p. 66; and *Tallinn Manual 2.0…, op. cit.,* rule 69, par. 5

[964] ILC, "Draft Articles on responsibility of States…", *op. cit*., 2001, vol. II, part 2.

[965] *Ibid*, Commentary (1), p. 47.

[966] *Tallinn Manual 2.0…, op. cit.,* rule 70.

[967] SCHMITT, M. N., "*Cyber operations …*", *op. cit*., p. 153.

In order for a threat of force to constitute a violation of International Law, it must be known and clearly identifiable by the target State[968]. In this regard, it seems that "the introduction into a State cyber system of vulnerabilities which are capable of destructive activation at some later date would not constitute a threat of the use of force unless their presence is known to the target State and the originating State exploits them for some coercive purpose"[969].

Also, the relationship between the concerned States has a fundamental role in determining whether the target State is entitled to feel threatened or the conduct can be qualified as threat of force. In this sense, "although threats are usually intended to be coercive in effect, there is no requirement that specific 'demand' accompany the threat"[970]. In this regard, the *Independent Fact-finding Mission on the Conflict in Georgia* affirmed that "as soon as {militarized acts} are non-routine, suspiciously timed, scaled up, intensified, geographically proximate, staged in the exact mode of a potential military clash, and easily attributable to a foreign-policy message, the hostile intent is considered present and the demonstration of force manifest"[971]. It means that, in each case, to find out the existence of a threat of use of force by cyber operations, it is necessary to examine the several factors involving the potential threat of force.

Those actions that simply threaten the security of the target State without communicative in nature cannot constitute threat of force. For instance, when there are high tensions between two States and one of them aggressively begins developing the capabilities necessary to conduct massive malicious cyber operations against the other, the mere acquisition of such capabilities that could be used to conduct activities employing the use of force cannot constitute a threat[972].

---

[968] ROSCINI, M., *Cyber operations…, op. cit.*, p. 68.

[969] SCHMITT, M. N., "Cyber operations*…", op. cit.*, p. 153.

[970] *Tallinn Manual 2.0, op. cit.,* rule 70, par. 4.

[971] IIFFM, *Report on the conflict in Georgia*, vol. II, September 2009, p. 232.

[972] *Tallinn Manual 2.0, op. cit.,* rule 70, par. 4.

One of the problems is whether a State lacking cyber capabilities to carry out its threat can violate the prohibition of threat of force. It must be pointed out that cyber capability is not as dependent on a State's size or economic and military capacity as it is the capacity to use conventional force. It means that it may be more difficult for a State to evaluate the capacity of another State to carry out its cyber threats. Thus, the cyber capability of one State plays a minor role in assessing the cyber threats[973].

Another controversial issue is regarding a State that possesses the capability to carry out the threat but clearly has no intention of doing so. For instance, a leader of a State with high offensive cyber capabilities who threatens another State just for reasons of domestic affairs[974].

Thus, in the context of cyber attacks, in practice, it seems more difficult to notice the existence of a threat of force than in the case of a threat by conventional means; first, because an unlawful threat of cyber attack is not visible since it cannot be depicted from the preparation until the conduct of the cyber attack; second, the threat is more independent from the cyber capability of the State than from the threat by conventional force; and third, noticing the existence of intentions in cyber attacks the same way as in conventional force is really complex.

3. *Cyber operations below the level of the prohibition of the use of force*

Certain categories of coercive operations (political or economic coercion) cannot fall in the scope of the prohibition of the use of force. Similarly, some cyber operations analogous to political or economic coercion are below the level of the use of force[975]. As mentioned in the First Chapter, the drafting of the UN Charter and the proceedings leading to the UNGA Resolution 2625 (XXV), the political and economic coercions were rejected to be included in the scope of the principle of the prohibition of the use of force. Therefore, those kinds of cyber operations that intent to coerce politically or economically do not violate the

[973] *Ibid,* rule 70, par. 5.

[974] *Ibid,* rule 70, par. 6.

[975] *Ibid*, rule 69, par. 2

principle of the prohibition of the use of force[976]. Then, this view poses obscuration in an *effect-based* (result-oriented) approach, because it blurs the distinction between the economic effects and the traditional view of the use of force which is characterized by armed force, particularly, when economic coercion has severe disruptive and destructive effects[977].

In this regard, *Tallinn Manual 2.0* reaffirms that "neither non-destructive cyber psychological operations intended solely to undermine confidence in a government, nor a State's prohibition of e-commerce with another State designed to cause negative economic consequences, qualify as uses of force"[978]. In the same line, *Chatham House* named economic or trade injury as *computer network interference,* rather than attacks that are more closely associated with military category[979]. However, "some may categorize massive cyber operations that cripple an economy as a use of force, even though economic coercion is presumptively lawful"[980].

In this regard, according to the UNGA Resolution 2131 (XX) on Declaration on the inadmissibility of intervention, to "use or encourage the use of economic, political or *any other type of measures* to coerce another State in order to obtain from it the subordination of the exercise of its sovereignty rights and to secure from it advantage of any kind"[981], can constitute a violation of the principle of non-intervention under the level of the use of force[982]. In this sense, the language of this Resolution is broad enough to include disruptive cyber attacks below the level of the use of force that may violate the principle of non-

---

[976] SCHMITT, M. N., "Cyber operations in International Law: the use of force, collective security, self-defence and armed conflicts", *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy,* 2010, p. 151-178, at p. 155.

[977] BARKHAM, J., "Information warfare…", *op. cit*., p. 86.

[978] *Tallinn Manual 2.0, op. cit.,* rule 69, par. 3.

[979] O'CONNELL, M., E., *et al*., "Cyber security and International Law", *International Law Meeting Summary, Chatham House*, 29 May 2012, p. 1-12, at p. 3.

[980] *Tallinn Manual 2.0, op. cit.,* rule 69, par. 10.

[981] UNGA, Resolution 2131 (XX), *op. cit,* par. 2 (italic is ours).

[982] see also ICJ, *Corfu Channel case*, *op. cit*, p. 35, in this sense, the ICJ declared that "It does not consider that the action of the British Navy was a demonstration of force for the purpose of exercising political pressure on Albania".

intervention. Thus, it seems that those cyber operations that clearly do not disrupt the critical infrastructures of another State cannot violate the principle of the prohibition of the use of force. In this context, some scholars assert that

> "just because a cyber attack or cyber espionage do not amount to an armed attack does not mean that International Law has no law against such wrongs. Interference with a State's economic sphere, air space, maritime space, or territorial space, even if not prohibited by article 2(4) of the UN Charter is prohibited under the general principle of non-intervention"[983].

In this regard, those cyber operations or cyber espionages that penetrate another State's economic sphere, air space, maritime space or territorial space without a critical disruption of its infrastructure breaches the principle of non-intervention.

Also, as we have seen *supra*, in accordance with the ICJ's judgment in the *Nicaragua case*, "the mere supply of funds to the *contras*, while undoubtedly an act of intervention in the internal affairs of Nicaragua, {...}, does not in itself amount to a use of force"[984]. Hence, the mere funding of hacktivist non-State actors to conduct cyber operations would not be a use of force[985].

Actually, not only cyber attacks that cause low-level disruption constitute intervention below the level of the use of force, "but also those that deface websites in order to foment civil strife in a State or the sending of thousand of e-mail to voters in order to influence the outcome of political election in another State"[986]; for instance, after the 2016 *US Presidential Election,* the *US* formally accused *Russia* of hacking the DNC's computer networks to interfere by releasing information about Clinton[987] In this sense, if such kind of

---

[983] O'CONNELL, M., E., *et al*., "Cyber security…", *op. cit*., p. 7.

[984] ICJ, *Nicaragua case, op. cit*., par. 228.

[985] *Tallinn Manual 2.0, op. cit.,* rule 69, par. 3.

[986] ROSCINI, M., *Cyber operations…, op. cit*., p. 65.

[987] MUELLER, R., "2016 Presidential Election Investigation Fast Facts", CNN, https://edition.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html, {18 March 2018}.

cyber operation is conducted, it can be understood as an interference below the level of the use of force[988].

Additionally, if a broadcast "is deliberately false and intended to produce dissent or encourage insurgents", or disseminates hostile propaganda and calumny, it would likely not reach to the level of use of force and would therefore be qualified in the frame of the principle of non-intervention[989].

In this context, it is valuable to refer to the cyber exploitation as a form of cyber activities that "includes the unauthorized access to other computer, computer systems and network to exfiltrate information, but without affection the functionally of accessed system or corrupting, amending or deleting the data resident therein", and that cannot constitute use of force[990]. Some cyber exploitations are a contemporary form of military reconnaissance or espionage. In fact, the aim of CNE operations can be stealing sensitive information from computer. Hence, these activities can not constitute use of force because, as we said, espionage is not in prohibited in International Law[991]. In other words, "espionage activities conducted by clandestine agents are merely unfriendly acts"[992]. In this regard, *Tallinn Manual* 2.0 reaffirms that computer networking exploitation is a pervasive tool of modern

[988] The UK Attorney General Jeremy Wright QC MP expressed that "cyber operations to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of parliament {…} such acts must surely be a breach of the prohibition on interventions in the domestic affairs of States", see UK Attorney General Jeremy Wright QC MP, "Cyber and International Law in the 21st century", available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century , {visited on 23 May 2018}.

[989] JAMNEJAD, M.; WOOD, M. "The principle of non-intervention", *LJIL*, 22(2), 2009, p. 345-381, at p. 374; and ROSCINI, M., *Cyber operations…, op. cit*., p. 65; see also UNGA Resolution 36/103 "Declaration on the inadmissibility of intervention and interference in the international affairs of States", of 9 December 1981; and view of a Group of legal scholars that assert that "propaganda, psychological operations, espionage, or mere economic pressure *per se*", can not constitute use of force, *Tallinn Manual, op. cit.,* rule 11, par. 9(h).

[990] ROSCINI, M., *Cyber operations…, op. cit*., p. 65.

[991] *Ibid*, p. 66. *Tallinn Manual 2.0, op. cit.,* rule 32, par. 6.

[992] DINSTEIN, Y., Computer network attacks…, *op. cit*., p. 105; and NAVARRETE, I., "L'espionnage en temps de paix en Droit International Public", *CYIL*, 53, 2015, p. 1-65, at p. 61-63.

espionage; some actions, such as the disabling of cyber security mechanisms in order to monitor keystrokes, despite their invasiveness, are unlikely to be seen as a use of force[993].

Most of cyber intrusions for the purpose of espionage or theft are classified as CNE while the rest are categorized as CNA. In this way, *Trap doors* and *Sniffers* are particular tools for cyber espionages. *Trap doors* allows an external user to access software at any time without the computer owner being aware of while *Sniffers,* by means of a remote computer, record data by passing over the network to steal user IDs and passwords. This kind of operations are not prohibited in International Law but are usually unlawful at the domestic level[994]. It is important to point out that although espionage is not prohibited in International Law *per se*, it does not mean that cyber espionage never qualifies as use force, especially when it damages cyber infrastructures that causes technical malfunction[995].

C. **Cyber operations as an armed attack in the context of the right of self-defence**

As we have seen, a cyber operation can fall under the prohibition of the use of force. In this sense, in order to justify the right of self-defence against a cyber attack, some requirements must be met. First, it is necessary to find out if such cyber attack can constitute an armed attack to allow a victim State to exercise the right of self-defence; and second, how to match the other requirements relating the exercise of the right of self-defence (necessity, proportionality and immediacy) with a cyber attack when it amounts to an armed attack.

Before going, we must point out that States are the only subjects that enjoy the right of self-defence. However, if private entities, such as corporations, are subject to a hostile cyber attack they cannot respond by invoking the right of self-defence, regardless of its severity; "their responses would be governed by domestic and International Criminal Law norms"[996].

---

[993] *Tallinn Manual 2.0 …, op. cit.,* rule 69, par. 9(d).

[994] ROSCINI, M., "World wide warfare…", *op. cit.*, p. 93.

[995] *Tallinn Manual 2.0, op. cit.,* rule 69, par. 9(d).

[996] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 163.

1. *Cyber operations as an armed attack by States*

The scientific and technological revolution has "changed the scope and pace of battle"[997]. Nowadays, all computer servers can work as an instrument of command control, communications and intelligence, and "the modern computer can also become a weapon in itself by being aligned for attack against other computer systems serving the adversary"[998]. Hence, it arises the question of whether some cyber operations can be qualified as an armed attack to justify the right of self-defence.

a) *Cyber operations as an armed attack*

As we have seen, according to article 51 of the UN Charter, nothing "shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a member of the United Nations". But International Law does not explain precisely what constitutes an armed attack.

One of the instruments that helps identifying the armed attack is the UNGA Resolution 3314 (XXIX) on the definition of aggression. Even though this Resolution does not define armed attack, it provides examples of actions that can be considered an armed attack; for instance, article 3(b), which refers to "the use of *any weapons* by a State against the territory of another State"[999]. It seems that its language is sufficient to cover cyber attacks[1000].

Moreover, in the *Nicaragua case* the ICJ, by referring to such Resolution, indicates that the notion of aggression is broader than the notion of armed attack[1001], and affirmed that there is not definition of *armed attack* in the UN Charter[1002]. Determining whether an armed

[997] SCULLEY, J. R., "Computers, military use of", in DUPUY, T. N. (ed.), *International military and defense encyclopedia*, Potomac Books, 2, 1993, p. 617.

[998] DINSTEIN, Y., "Computer network…", *op. cit*., p. 102.

[999] UNGA Resolution 3314 (XXIX), op. cit., (italic is ours).

[1000] ROSCINI, M., *Cyber operations…, op. cit*, p. 72

[1001] ICJ, *Nicaragua case, op. cit*., par. 195.

[1002] *Ibid*, par. 176.

attack has taken place "does not necessarily depend on the choice of weapons by the attacking party"[1003]. Again, it is important to emphasise that, in accordance with ICJ's view, article 51 does not refer to specific weapons and applies to any armed attack, "regardless of the weapons employed"[1004].

In this field, international community generally accepts *Pictet's* scope, duration and intensity test as the starting point for evaluating whether a certain use of force constitutes an armed attack. Following Pictet's test, "a use of force is an armed attack when it is of sufficient scope, duration, and intensity"[1005]. In this context, both States and the ICJ have frequently applied this guidance in the field of conventional understanding of the use of force. According to the majority of scholars, intuitively a cyber attack can constitute an armed attack, especially when it may cause injury or death. Nevertheless, part of the legal community is reluctant to classify cyber attacks as armed attacks because they do not resemble to "classical attack with traditional military force"[1006].

As has been observed in Brownlie's view, biological and chemical attacks can constitute use of force, because of the *destruction of life and property*[1007]. In this respect, if the international community is under the *effect-based* approach, it accepts chemical, biological or radiological attacks as armed attacks. Similarly, a cyber attack can constitute an armed attack[1008]. In other words, the fact that a cyber attack does not use traditional kinetic weapons does not necessarily mean that it cannot be an *armed attack*. Thus, from a legal perspective "there is no reason to differentiate between kinetic and electronic means of

---

[1003] DINSTEIN, Y., "Computer network…", *op. cit*., p. 103.

[1004] ICJ, *Legality of nuclear weapon, op. cit*., par. 39.

[1005] CARR, J., *Inside cyber warfare..., op .cit.,* p. 58; HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense against cyber-attacks and the shockwaves in the legal community: one more reason for holistic legal approach to cyberspace", *Mediterranean Journal of Social Sciences*, *4*(14), 2013, , p. 115-124, at p. 117; and SHARP, W, G., *Cyberspace..., op. cit.,* p. 60-61.

[1006] WINGFIELD, TH., *When is a cyber attack an 'armed attack'?: legal thresholds for distinguishing military activities in cyberspace*, Cyber Conflict Studied Association, 2006, p. 6.

[1007] BROWNLIE, I., *International law…, op. cit*., p. 362.

[1008] PETRAS, C. M., "The use of force in response to cyber-attack on commercial space systems-reexamining self-defense in outer space in light of the convergence of us military and commercial space activities", *Journal of Air Law and Commerce*, 67, 2002, p. 1213-1268, at p. 1259.

attack. A premeditated destructive CNA can qualify as an armed attack just as much as a kinetic attack bringing about the same-or similar–results"[1009]. In addition, Zemanek remarks that

> "it is neither the designation of device, nor its normal use, which make it a weapon but the intent with which it is used and its effect. The use of any device, or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfil the conditions of an *armed* attack"[1010].

This view is implicitly supported by the UNSC Resolutions 1368 and 1373 in 2001, where they advocate to the right of self-defence in response to the hijacked air planes after the events of 11 September 2001[1011]. Likewise, this approach explicitly appears in *Tallinn Manual 2.0* where it affirms that "A State that is the target of cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence"[1012].

It seems that the point of view that a cyber operation can be qualified as an armed attack is accepted by some States. In this sense, the US *International Strategy for Cyberspace* in 2011 states that "consistent with the United Nations Charter, States have an inherent right to self-defence that may be triggered by certain aggressive acts in cyberspace"[1013]. Likewise, the *Department of Defense Cyberspace Policy Report* in 2011 reaffirms that "we {US} will respond to hostile acts in cyberspace as we would to any other threat to our country"[1014]. Additionally, the *Presidential Policy Directive 20* more explicitly asserts that "the United

---

[1009] DINSTEIN, Y., "Computer network attacks…", *op. cit*., p. 103.

[1010] ZEMANEK, K., "Armed attack", in *Max Planck Encyclopedia of Public International Law*, 2013, par. 21, available at http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241 {visited on 22 June 2018}.

[1011] ROSCINI, M., "World wide warfare…", p. 115.

[1012] *Tallinn Manual 2.0…, op. cit.,* rule 71.

[1013] US, *International Strategy for Cyberspace, op. cit*., p. 10.

[1014] US, DoD CYBERSPACE POLICY REPORT, *A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, November 2011, p. 2, available at https://assets.documentcloud.org/documents/266862/department-of-defense-cyberspace-policy-report.pdf,]visited on 22 February 2018[.

States government shall reserve the right to act in accordance with the United States inherent right of self-defence as recognized in International Law, including through the conduct of DCEO {Defensive Cyber Effects Operations}"[1015]. Furthermore, a legal advisor of the US *Department of State* proclaims that "A State's national right of self-defence, recognized in article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack on an imminent threat thereof"[1016]. Thus, the US clearly asserts that it will treat cyber attacks the same way as conventional attacks[1017].

The UK reorganized cyber space as a fundamental element of national security and international infrastructures[1018] and declared that "the UN Charter applies in its entirety to State actions in cyberspace, including the prohibition of the use of force (article 2(4)), the peaceful settlement of disputes (article 33), and the inherent right of States to act in self-defence in response to an armed attack (article 51)"[1019].

In the same direction, the *Armed Forces of the Russian Federation* claims the right of self-defence "with the implementation of any chosen options and means" in conformity with International Law[1020]. Moreover, the *White Paper on German Security Policy* suggests that indirect military attack from or on cyber space against German critical infrastructure can

---

[1015] US, *Presidential Policy Directive/PPD-20*, *op. cit*., p. 6.

[1016] KOH, H. H., "International Law…", p. 4.

[1017] DEWEESE, G. S., "Anticipatory and preemptive self-defense in cyberspace: the challenge of imminence", in MAYBAUM, M., *et al*., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace,* NATO CCD COE, 2015, p. 81-91, at p. 82.

[1018] UK, *National Cyber Security Strategy 2016-2021*, October 2016, p. 39, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf,]visited on 4 March 2018[; see also UK and Northern Ireland views in UNGA Resolution A/72/315 "Developments in the field of information and telecommunications in the context of international security: report of the Secretary–General", 11 August 2017.

[1019] UK, FOREIGN AND COMMONWEALTH OFFICE, "Response to General Assembly Resolution 71/28 'Developments in the field of information and telecommunications in the context of international security'", July 2017, available at https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/09/UK-ES-and-full.pdf, [visited on 22 June 2018].

[1020] *Conceptual views on the Activities of the armed forces of the Russia Federation in the information space*, of 9 September 2000, p. 12, available at http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, {visited on 29 April 2018}.

be countered using military means[1021], and recently, the German Government explicitly maintained that "the Federal Republic could react to this {cyber operation} with all permissible military means"[1022]. Also, the Dutch *Advisory Council on International Affairs* remarks that "States that seriously, organized cyber attack on essential functions of the State could conceivably be qualify as an 'armed attack' within meaning of article 51 of the UN Charter"[1023]; and the Italian Government noticed that States may protect national critical infrastructure from any external attacks in a consistent manner with International Law[1024].

In fact, the view of these States has been explicitly expressed by the UN *Groups of Governmental Experts* (GGEs) that examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them since 2004. The UN GGEs in 2013 in reaction to the threats of cyber technologies affirmed that International Law, and particularly the UN Charter, is applicable and is essential to maintaining peace and stability and promoting accessible and peaceful cyber environment. This GGEs report was adopted by Resolution 68/243[1025] and requested the UNSG to establish a new GGE to provide a report to UNGA in 2015. That year, the new Group with 20 experts, including the UK, the US, Russia and China reaffirmed that "the inherent right of States to take measures consistent with International Law and as recognized in the Charter" [1026]. This position was adopted by the UNGA[1027]. Hence, the GGEs explicitly emphasized that the right of self-

[1021] F. R. GERMANY, FEDERAL MINISTRY OF DEFENSE, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, 2006, p. 19, available at http://responsibilitytoprotect.org/Germany_White_Paper_2006.pdf, [visited on 1 January 2018].

[1022] GERMAN GOVERNMENT "German could dispatch armed forces in response to cyberattacks", 6 Jun 2018, available at https://global.handelsblatt.com/politics/germany-soldiers-combat-cyberattacks-931929, {visited on 25 June 2018}.

[1023] DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare…, op. cit*., p. 21.

[1024] GOVERNO ITALIANO, *La posizione italiana sui principi fondementali di internet*, of 17 September 2012, p. 5, available at http://download.repubblica.it/pdf/2012/tecnologia/internet.pdf, [visited on 25 May 2018].

[1025] UNGA, Resolution A/68/243 "Group of governmental experts on developments in the field of information and telecommunications in the context of international security", 27 December 2013.

[1026] UNGA, Doc. A/70/174 "Group of governmental experts on developments in the field of information and telecommunications in the context of international security", 22 July 2015, par. (c), p. 12.

[1027] UNGA, Doc. A/70/172 on "Developments in the field of information and telecommunications in the context of international security", 22 July 2015.

defence is applicable in response to cyber operations when they reach the level of an armed attack[1028].

In the same line, the NATO, on 5 September 2014, approved a new *Enhanced Cyber Defence Policy* which recognized that the cyber attack can trigger the obligation under article 5 of the NATO Charter, affirming that "cyber defence is part of NATO core task of collective defence"[1029].

Nevertheless, some scholars maintain that translating existing rules of jus *ad bellum* to the cyberspace activities produces extensive uncertainty. In this sense, they assert that cyber attack alone cannot constitute an armed attack for the purpose of article 51 when "it {cyber attack} lacks the physical characteristics traditionally associated with military coercion"[1030]; also, they allege that "international laws associate with the use of force are woefully inadequate in terms of addressing the threat of cyber warfare"[1031]. Others note that "attempting to apply these conditions to cyber force actions is difficult, if not impossible"[1032].

Thus, even the uncertainty in the applicability of existing International Law to cyber operations, those States targeted by cyber attacks are allowed to respond forcibly in the right of self-defence if such attacks reach the threshold of an armed attack[1033]. So far, although we have not experienced severe cyber attacks that cause death and significant material property damages as to be qualified as armed attacks[1034], it does not mean that

---

[1028] The UK Attorney General Jeremy Wright QC MP, "Cyber and International Law…", *op. cit*.

[1029] NATO, *Wales Summit Declaration*…, *op. cit*., par. 72.

[1030] HOLLIS, D. B., "Why States need an International Law for information operations", *Lewis & Clark Law Review,* 11, 2007, p. 1023-1061, at p.1023-1042; see also KANUCK, S. P., "Information warfare: new challenges for Public lnternational Law", *HILJ,* 37, 1996, p. 272-289, at p. 288-289.

[1031] ADDDICOTT, J. F., "Cyberterrorism: legal policy issues", in MOORE, J. N., *et al*. (eds.), *Legal issues in the struggle against terror*, Carolina Academic Press, 2010, p. 519-566, at p. 550.

[1032] O'CONNELL, M., E., *et al*., "Cyber security…", *op. cit*., p. 6.

[1033] Among others, RATNER, S. R., "Self-defense against terrorists...", *op. cit*., p. 18; REMIRO, A., *et al*., *Derecho Internacional*, *op. cit*., p. 690; ROSCINI, M., *Cyber operations..., op. cit*., p. 71; and CERVELL, M. J., *La legítima defensa..., op. cit.,* p. 302.

[1034] Cyber attack in Estonia (2007), Georgia (2008), Iran (2010), Myanmar (2010), US (2011) or Middle East (2012).

cyber operations or series of such operations cannot constitute an armed attack in International Law[1035]. In this respect, the ILA affirms that "an emerging view is that cyber operations may constitute an armed attack if their scale and effects mirror those of a traditional kinetic attack"[1036].

In relation to the question of whether the right of self-defence is applicable to cyber operations by accidental victim (without intention), there have always been serious controversies. The majority of experts of the *Tallinn Manual 2.0* believe that "intention is irrelevant in qualifying an operation as an armed attack and that only the scale and effects matter"[1037]. However, they emphasise that any response would have to be adopted with the necessity and proportionality criteria; in this regard, all the experts agreed that a lawful reaction would be determined by reasonableness of the State's assessment as to whether an armed attack is underway against it[1038]. Therefore, they mention the case of a cyber armed attack by State A against State B that include bleed-over effects (with enough scale and effect criteria to be an armed attack) to State C, State C is entitled to resort to the use of force in self-defence[1039]. In fact, this part of doctrine focuses more on the consequences of the attack[1040] rather than on the object of the attack or the intention of the attacker.

However, some experts of *Tallinn Manual* affirm that intention is necessary to characterize a cyber operation as an armed attack[1041]. In this sense, it is important to point out that the ICJ declared that an armed attack must be carried out "with the specific intention of harming"[1042]. Also, it seems that the intention[1043] can be implicitly derived from article

---

[1035] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit*, p. 119.

[1036] ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 18.

[1037] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 14.

[1038] *Ibid;* see also PERT, A., "Proportionality in self-defence...", *op. cit*., p. 75.

[1039] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 15; and SCHMITT, M. N., "Cyber operations…", *op. cit*., p. 165.

[1040] SCHMITT, M. N., "Computer network attack…", *op. cit.,* p. 911.

[1041] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 14.

[1042] ICJ, *Oil platform case, op. cit*., par. 64.

[1043] *Animus aggressionis is* defined as "a deliberate intention to cause damage to property, people or systems of a certain State", ROSCINI, M., *Cyber operations…, op. cit*., p. 77.

3(f)) of the UNGA Resolution 3314 (XXIX) on the definition of aggression, where, in order to an action from the territory of one State to constitute an aggression, it is necessary that such State *allows* its territory to carry out such action. To assess the hostile intention in the cyber operations, the US specifies that it derives from "such factors as persistence, sophistication of methods used, targeting of especially sensitive system and actual damage done"[1044].

In this sense, Roscini states that if an armed attack by State A against State B additionally constitutes unintended harmful consequence on property persons or systems of State C, "a reaction in self-defence by State C would not be necessary, as State A will probably stop the attack on C"[1045]. Also, Sharp advocates to the application of hostile intent as a basis for a victim State's response[1046]. Then, to our understanding, there must be hostile intention as criteria to qualify a cyber operation to an armed attack.

Furthermore, this approach is more compatible with the purpose *of maintaining international peace and security* established in article 1(1) of the UN Charter because, if the hostile intention is required, it restricts the possibilities to resort to the right of self-defence to solve any international controversies. In the case of lack of intention by the attacking State, it would be more suitable to apply other mechanisms, like countermeasures[1047], which would be more easily consistent with the plea of necessity. In this sense, a State can take any responsive actions that do not amount to a use of force; for instance, a State may choose to block incoming cyber transmissions emanating from a State that has used force against it[1048].

[1044] US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment…*, *op. cit.*, May 1999, p. 21.

[1045] ROSCINI, M., *Cyber operations…, op. cit.*, p. 77

[1046] SHARP, W. G., *Cyberspace…, op. cit.,* p. 132-133; and JENSEN, E.T., "Computer attacks on critical national infrastructure: a use of force invoking the right of self-defense", *Stanford Journal of International Law,* 38, 2002, p. 224.

[1047] See O'CONNELL, M., E., *et al.*, "Cyber security…", *op. cit.*, p. 8.

[1048] SCHMITT, M. N., "Cyber operations*…", op. cit.*, p. 159.

b) *Cyber operations that amount to an armed attack*

As has been seen *supra*, an armed attack is a use of force with enough graveness that is originated outside the territory of the target State; then, "an armed attack must have a trans-border element"[1049]. In this sense, in the field of cyber operations, Dinstein asserts that "International Law come into play only at a point when the CNA turns into a cross-border operation"[1050]. Hence, cyber operations can become an armed attack when a State directly or indirectly engages in cyber operation against another State[1051].

Contrary to the principle of the prohibition of the use of force where the term *use of force* is interpreted leeway to include non-necessarily kinetic actions, the term *armed attack* tolerates little interpretive latitude to avoid abuses of article 51 as an exception to the principle of the prohibition of the use of force[1052].

In the field of cyber operation, Greenwood, former judge of the ICJ, states that any assertion towards considering cyber attacks as armed attacks should be "treated with considerable caution" and taken seriously. In this sense, he remarks that

> "The planning of virus or the use of other computer techniques to undermine, for example, the computer systems regulating a State's financial system or immigration controls are difficult to see as an armed attack. Although, the consequences of such conduct may be very serious, it seems closer to the concept of economic coercion. On the one hand, if such action were used to produce results similar to those which could otherwise be achieved only by the use of armed force, for example, causing aircraft to crash or dams to open

[1049] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 3.

[1050] DINSTEIN, Y, "Computer network attacks…", *op. cit.*, p. 103.

[1051] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 3.

[1052] WAXMAN, M. C., "Cyber attacks and the use of force…", p. 427; SCHMITT, "Cyber operations…", *op. cit.*, p. 163; and FRANK, Th. M., *Recourse to force: State actions against threats and armed attacks*, CUP, 2002, p. 45-52.

and flood areas of a State's territory, then the argument that such action should be treated as a form of armed attack is more plausible"[1053].

Hence, he takes a cautious view to considering all cyber attacks as armed attacks. In this point of view, only under exceptional circumstances, when the results of the cyber attacks are similar to the result of the armed forces it can be considered an armed attack.

Also, in this context, O'Connell points out that "Not only must there be an armed attack or armed attack equivalent to justify the use military force in self-defence, but the attack must be significant"[1054].

As we have seen, there is a distinction between *the most grave forms* (armed attack) from other *less grave forms of use of force*[1055]. Given the lack of a clear definition of graveness, *scale and effects* are the criteria to distinguish armed attack from other uses of force[1056]. Then, in conformity with the *effected-based* approach, the qualification of a cyber operation as an armed attack depends on its scale and effects[1057]. In other words, "use of force is an armed attack when its scale and effects are grave enough"[1058]. In this sense, the disruption of communications and digitized services through the induced failure of computer systems without any human casualties or significant destruction of property "does not entail sufficient grave consequences" to constitute an armed attack[1059]. Moreover, this approach is confirmed in *Tallinn Manual 2.0* where "a cyber operation that seriously injures or kills a

[1053] GREENWOOD, Ch., "Self-defence", in *Max Planck Encyclopedia of Public International Law*, 2011, par. 14, available at http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401?prd=EPIL, {visited 22 June 2018}.

[1054] O'CONNELL, M., E., *et al*., "Cyber security…", *op. cit*., p. 6.

[1055] ICJ, *Nicaragua case, op. cit*., par. 191.

[1056] *Ibid*, par. 195;, see also RUYS, T., *'Armed Attack'..., op. cit.,* where affirms that *scale* refer to amount of armed force employed or its duration and *effect* to damage cause, p.139.

[1057] SCHMITT, "Cyber operations…", *op. cit*., p. 163.

[1058] ROSCINI, M., *Cyber operations..., op. cit*., p. 71.

[1059] DINSTEIN, Y., "Computer network attacks…", *op. cit*., p. 105.

number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement" can constitute an armed attack[1060].

Nowadays, it is not clear the extent of death, damage, destruction or suffering of cyber operation to constitute an armed attack. This issue remains unsettled in *Tallinn Manual 2.0* where there are serious controversies on those cyber operations that do not result in injury, death, damage or destruction, but they have extensive negative effects that can constitute an armed attack. In this regard, in *Tallinn Manual 2.0* some experts assert that "a cyber operation directed against a State's critical infrastructure that causes severe, albeit not destructive, effect would qualify as an armed attack"[1061]. Similarly, some scholars refer to "operation that cause or is reasonably likely to cause extrinsic physical damage to persons or properties or severe disruption of critical infrastructures"[1062]. Hence, the mere "stealing sensitive military information without immediate loss of life or destruction result" or cyber operations that cause "cut off a country of internet without physical damage and sever incapacitation of essential service" cannot be qualified as an armed attack[1063].

The cyber attacks on State military infrastructures can be an armed attack *per se* if such attacks disable a State's command and control in a way that causes massive disruption (disabling the decision making hard core of the State), even if those attacks did not cause grave harm (physical damage) that debilitates the State. Thus, in order for a cyber attack to constitute an armed attack, material and human harm is not necessary since the massive disruption that debilitates the State would be enough[1064].

Furthermore, according to article 3(f) of the UNGA Resolution 3314 (XXIX) on the definition of aggression, it is noticeable that if a State knowingly allows another States to

---

[1060] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 8.

[1061] *Ibid,* par. 12.

[1062] ROSCINI, M., *Cyber operations…, op. cit*., p. 71.

[1063] *Ibid*, p. 71-72; see also SCHMITT, "Cyber operations…", *op. cit.*, p. 164.

[1064] TSAGOURIAS, N., "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict and Security Law,* 17(2), 2012, p. 229-244, at p. 232.

use its cyber infrastructure to launch cyber operations which are qualified as acts of aggression, they would not necessarily be qualified as armed attacks[1065].

In relation to find out what effects lead to assessing a cyber action as an armed attack, *Tallinn Manual 2.0* states that "all reasonably foreseeable consequences of cyber operation" can be taken into account to qualify such operation as an armed attack. For instance, those cyber operations that target a water purification plant whose sickness and death is foreseeable by its drinking[1066]. Also, Dinstein adds that "fatalities caused by loss of computer-controlled life-support systems; {...} shut down of computers controlling waterworks and dams, generating thereby floods of inhabited areas" and the more flagrant case "the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated", would be qualified as an armed attack[1067].

Moreover, the NATO, in its *Enhanced Cyber Defence Policy,* recognized that "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"[1068]. In any case, it is important to point out that the amount of fatalities depend on the scientific and technological development of each State; this means that States with more computer dependency would be more vulnerable[1069].

According to International Law, low-level attacks do not amount to an armed attack, but when there is an underlying strategy behind the low-intensity attacks and their cumulative effects are considered we reach a different conclusion. In this sense, it seems that series or accumulation of cyber incidents below the threshold of an armed attack can amount to an armed attack; for instance, while frequent-albeit mildly disruptive attacks on a State's financial system may cause limited damage, the accumulation of such damages may be

[1065] ROSCINI, M., *Cyber operations…, op. cit.*, p. 72.

[1066] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 13.

[1067] DINSTEIN, Y, "Computer network attacks…", *op. cit.*, p. 105.

[1068] NATO, *Wales Summit Declaration…*, *op. cit.,* par. 72; see also, *Tallinn Manual 2.0*, *op. cit.*, rule 14, par. 9.

[1069] NATO, *ibid.*; see also WAXMAN M. C., "Cyber-attacks and the use of force…", *op. cit.,* p. 424.

substantial if the overall trust in the system is destroyed, which may have been the hostile intention of the minor attacks all along. In some cases, "the accumulation of minor cyber provocations could rise to level of an armed attack for self-defence purposes"[1070]. In other words, it is widely accepted that

> "the determinative factor is whether the same originator (or originators acting in concert) has carried out smaller-scale incidents that are related and that taken together meet the requisite scale and effects. If there is convincing evidence that this is the case, there are grounds for treating the incidents as a composite armed attack"[1071].

Regarding the *accumulation theory*, in order for cyber operations to amount to an armed attack, it is not necessary to account only minor cyber attacks individually since they can be combined with other armed forces, such as military. In this sense, "cyber operation that accompany military action otherwise constituting an armed attack have no bearing on the nature of attack"[1072]; for example, where cyber attacks likely conduct against enemy command or air control defence system as an element of a broader military operation, regardless of considering whether they are independently qualified as an armed attack, they can be responded in self-defence, since such cyber attacks are a component of the overall military operation[1073].

Hence, an armed attack can be carried out in various ways, from full scale invasion to a series of small-scale uses of force in the same offensive to the same target; then, if cyber operations do not amount, individually or accumulatively, to an armed attack, the victim State does not have the right to respond forcefully to such cyber operations.

[1070] TSAGOURIAS, N., "Cyber attacks...", *op. cit.*, p. 233.

[1071] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 11.

[1072] SCHMITT, "Cyber operations…", *op. cit.*, p. 164.

[1073] *Ibid*.

c) *Infrastructures and those damages that can be object of cyber attacks*

On reliance to modern society on computer system and networks, cyber technologies from one State can produce substantial disruption to another State, being that analogous to the use of kinetic weapons without physical damage. In this regard, it is unreasonable to accept the idea that those cyber operations as CNA that "does not physically destroy the object of attack in the traditional sense, it can never amount to use of force or an armed attack"[1074]. In this regard, the nature of the target is vital to determine whether a cyber operation amounts to the level of an armed attack to justify the exercise of the right of self-defence[1075].

To illustrate the nature of such vital and sensitive system, the US *Executive Order 13,010* of 1996 emphasized on the significant importance the computer networks have had for the national security, affirming in broad terms that

> "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, water supply systems, emergency services (including medical, police, fire, and rescue) and continuity of government" [1076].

In this direction, Sharp asserts that "any computer network attack {conducted by a State} that internationally caused any destructive effect within the sovereign territory of another

[1074] JENSEN, E.T., "Computer attacks on critical national infrastructure: a use of force invoking the right of self-defense", *Stanford Journal of International Law,* 38, 2002, p. 207-240, at p. 222.

[1075] *Ibid*, p. 226.

[1076] US, *Excusive Order No. 13010*, "Critical Infrastructure Protection", 15 July 1996, 61(138), *Federal Register*, 17 July 1996, p. 37347, available at https://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf, [visited on 3 April 2018].

State is an unlawful use of force that may constitute an armed attack prompting the right of self-defence"[1077].

However, it is difficult to accept the idea that mere unauthorized intrusions into unclassified information system (for instance, espionage) can constitute an armed attack[1078].

Following the field of cyber attacks, even theoretically, the economic coercion cannot be an armed attack. If a cyber operation is precursor of an imminent armed attack, in extreme situations, it can constitute an armed attack. In this sense, *Chatham House Principles* asserts that

> "An armed attack involves the use of armed force and not mere economic damage. Economic damage, for example, by way of trade suspension, or by use of a computer virus designed to paralyse the financial operations of a State stoke exchange or to disable the technology used to control water resources, may have a devastating impact on the victim State but the principles governing the right of to use force in self-defence are confined to a *military* attack. A purely, 'economic' attack might however give rise to the right of self-defence if it precursor to an imminent armed attack"[1079].

Hence, cyber operations which cause physical damage to critical infrastructures of States or severely disrupt the functioning or incapacitate such infrastructures can potentially constitute an armed attack. It means that the destruction or the disruption of critical infrastructures can constitute an armed attack to allow the exercise of the right of self-defence if they have enough graveness[1080]. Then, the scale, scope and duration of the consequences will be relevant to assess the severity[1081]. However, it is necessary to

---

[1077] SHARP, W. G., *Cyberspace…, op. cit*., p. 223.

[1078] US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment…*, *op. cit*., May 1999, p. 18.

[1079] *The Chatham House principles*…, p. 965.

[1080] ROSCINI, M., *Cyber operations…, op. cit*., p. 75-76.

[1081] SCHMITT, "Cyber operations…", *op. cit*., p. 156; and JENSEN, E.T., "Computer attacks…", *op. cit*., p. 224.

emphasize that when passive cyber defences[1082] are reasonable, effective and proportionate means to react to the purpose of repelling the attack, even if the disruptive cyber operation amounted to an armed attack, it is not possible to resort to the right of self-defence[1083].

According to Dinstein, some operations, such as the "disruption of communications and digitized services through the induced failure of computer systems, without causing human casualties or significant destruction of property {that} does not entail sufficiently grave consequences" (like espionage), do not constitute an armed attack[1084]. However, he adds that some computer operations that cause fatalities like "loss of computer-controlled life-support systems; extensive power grid outage (electricity blackout) creating considerable deleterious repercussions {…}", would be deemed to an armed attack[1085]. Therefore, it can be accepted that those cyber operations on critical State infrastructure which massively disrupt the apparatus of the State should be equated to an armed attack, even if it does not cause any immediate human injury or material damage[1086].

Nevertheless, in the field of critical infrastructure, it seems that there is not a general agreement on what type of infrastructures are critical. In this respect, the UNGA Resolution 58/199 states that "each country will determine its own critical information infrastructures"[1087].

In this sense, the States' approaches on the critical infrastructures are not identical. For instance, in 1999 the US DoD, *An Assessment of International Legal Issues in Information Operations,* refers to nation's air traffic control system, its banking and financial system and

---

[1082] Passive cyber defense include encryption, firewalls, and automatic detection; such measure are most effective when used in combination to form a *layered* security system; see JENSEN, E.T., "Computer attacks…", *op. cit.*, p. 230.

[1083] ROSCINI, M., *Cyber operations…, op. cit.*, p. 75.

[1084] DINSTEIN, Y., "Computer network attack…", *op. cit.*, p. 105.

[1085] *Ibid*.

[1086] TSAGOURIAS, N., "Cyber attacks…", *op. cit.,* p. 231, see also GILL, T. D; DUCHEINE, P. A. L., "Anticipatory self-defense in the cyber context", *International Law Studies*, 89, 2013, p. 438-471, at p. 445.

[1087] UNGA, Resolution 58/199 "Creation of a global culture of cybersecurity and the protection of critical information infrastructures", 23 December 2003.

public utilities and dams which are examples of critical infrastructures; if they are the target of a network attack and this finally leads to their shutdown, it entitles the victim State to use the right of self-defence[1088]. Also, the US *Patriot Act* of 2001 defines critical infrastructure as

> "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[1089].

Moreover, the *United States National Strategy to Secure Cyberspace* in 2003 describes critical infrastructures as

> "the physical and cyber assets of public and private institutions in {…} agriculture, food, water, public health, emergency services, government, defence industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping"[1090].

Nowadays, according to the US *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, approximately 85 percent of the US critical infrastructures and key assets are owned and operated by private industries[1091]; for instance, Glenny asserts that an attack to the US company Google, the most powerful presence on the

---

[1088] US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment…*, *op. cit.*, May 1999, p. 18.

[1089] US, *Patriot Act*, Public Law 107-599, section 1016, 26 October 2001, available at https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, [visited on 2 May 2018].

[1090] US, The *National Strategy to Secure Cyberspace*, The White House, February 2003, p. 1, available at https://www.nitrd.gov/cybersecurity/documents/NationalStrategytoSecureCyberspace2003.pdf, [visited on 2 January 2018].

[1091] US, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* The White House February 2003, p. 8, available at https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, [visited on 22 February 2018].

internet, would be an attack to the US critical infrastructure[1092]. While traditionally, these private operators have been responsible for protecting such physical assets against unauthorized intruders, currently they are not "designed to cope with significant military or terrorist threats, or the cascading economic and psychological impact they may entail"[1093].

In this viewpoint, the *Cyber Security Strategy of the United Kingdom* refers to nine essential services, such as energy, food, water, transport, communications, governmental and public services, emergency services, health and finance[1094].

Australia's *Cyber Security Strategy* proclaims its critical infrastructures as

> "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia ability to ensure national security", {in particular} "banking and finance, communications, emergency services, energy, food chain, health (private), water services, mass gatherings, and transport (aviation, maritime and surface)"[1095].

In addition, such strategy asserts that national interests "go beyond traditional notion of critical infrastructure and it includes any destruction which impact on Australia economic

---

[1092] GLENNY, M., "In America's new cyberwar google is on the front line", *The Guardian,* 18 January 2010, available at https://www.theguardian.com/commentisfree/2010/jan/18/america-cyberwar-google-china-computer, {visited 22 June 2018}.

[1093] US, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* The White House, February 2003, p. 8, *op. cit.*

[1094] UK GOVERNMENT, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, June 2009, p. 9, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf, [visited on 12 February 2018].

[1095] AUSTRALIAN GOVERNMENT, *Critical infrastructure resilience strategy*, 2010, p. 8, available at https://www.tisn.gov.au/Documents/+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf, [visited on 3 March 2018].

property, international competitiveness, public safety, social wellbeing or national defence and security" [1096].

In Russia's view, vital structures are

> "State's facilities, systems and institutions, deliberate influence on the information resource of which may have consequences that directly affect national security (transport, energy supply, credit and finance, communications, State administrative bodies, the defence system, law-enforcement agencies, strategic information resource, scientific establishments and scientific and technological governments, installations that pose heightened technological and environmental risks, and bodies for eliminating the consequences of natural disasters or other emergency situations"[1097].

Furthermore, Spain defines critical infrastructures as "the strategic infrastructures whose operation is indispensable and does not allow alternative solutions, for what their disturbance or destruction would have a serious impact on essential services"[1098].

The EU's Commission defines critical infrastructures as "those physical resources and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments"[1099].

[1096] *Ibid*, p. 12.

[1097] UNGA, *Developments in the field of information and telecommunications in the context of international security,* Report of the Secretary-General, Doc A/54/213, 10 August 1999, p. 10.

[1098] Article 2(e) of *Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas*, 28th April 2011; article 2(d) defines "Strategic infrastructures" as "the installations, networks, systems and physical equipment and information technology on which the operation of essential services rests".

[1099] EU, Communication from the Commission to the Council and the European Parliament*, Critical infrastructure protect in the fight against terrorism*, Doc COM, 2004, 702 final, 20 October 2004, p. 3, available at http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2004/0702/COM_COM(2004)0702_EN.pdf, [visited on 1 March 2018].

As a result, although there is not a general agreement to define critical infrastructure, the majority of States have accepted that certain services, such as security, food, water, transportation, banking and finance, health, energy, governmental and public services constitute critical infrastructures[1100]. Despite the different definitions there may be, "the minimum common denominator is that such infrastructures are vital for national security, including individual, societal, and governmental security"[1101]. Also, it is important to point out that nowadays critical infrastructures can include any essential governmental agencies as much as private companies. Hence, an armed attack can include cyber attack when it is directed against a State's critical infrastructure[1102] because, potentially, a cyber attack can severely cripple a State and undermine its political and economic affairs for a long time.

2. Cyber operations as an armed attack by non-State actors

Threats from subgroups and terrorist organizations are real and serious, and the vast majority of cyber operations against States are carried out by non-State actors[1103] because hacker tools are increasingly cheap, accessible and easy to 'weaponize'. Hence, destructive attacks can be perpetrated not only by nation-States, but also by national opposition groups, ideological radicals, terrorist organizations or individuals.

In this regard, since the events of 11 September, the international community is facing new challenges by non-State actors; on the one hand, their increasing willingness of killing massive numbers of people[1104] and, on the other hand, their extraordinary capacity to develop global networks and ability to conduct cyber operations[1105]. Hence, since the

---

[1100] TSAGOURIAS, N., "Cyber attacks…", *op. cit.*, p. 231.

[1101] ROSCINI, M., *Cyber operations…, op. cit.*, p. 58.

[1102] GILL, T. D; DUCHEINE, P. A. L., "Anticipatory self-defense…", *op. cit.*, p. 444.

[1103] ROSCINI, M., *Cyber operations…, op. cit.*, p. 80.

[1104] For instance, events of 11 September 2001in New York that killed 2,973 people; on 11 March 2004 in Madrid that killed 191 and wounded 2,050 people; or on 11 July 2006 bombing in the Mumbai train system that killed 209 and injured more than 700 people.

[1105] For example, recent studies indicate that *Al-Qaeda* has operated in a network in hundred countries, BAJORIA, J.; BRUNO, G., "Al-Qaeda (a.k.a. alQaida, al-Qa'ida)", *Council on Foreign Relations*, 6 June 2012,

effective employment of internet on the events of 11 September, non-State actors have had the ability to use computers to hijack satellites, provided that by "capturing signals beamed from outer space {it is alleged} terrorists could devastate the communications industry, shut down power grid, and paralyze the ability of developed countries to defend themselves"[1106]. In fact, the computer capability of *Al-Qaeda* is sufficient to kill substantial numbers of people with major property damage[1107].

As mentioned *supra*, the UN Charter does not expressly refer to the non-State actors as subjects of the provision of the principle of the prohibition of the use of force, and the right of self-defence is only justified against armed attacks that are directly or indirectly carried out by States. However, as we have seen, recent State practice shows that the international community has supported the use of the right of self-defence against non-State actors[1108].

In the context of cyber operations by non-State actors, the vast majority of the group of experts in *Tallinn Manual 2.0* asserts that

> "State practice has established a right of self-defence in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State, by non-State actors, such as terrorist or rebel groups. As an example {…} a devastating cyber operation undertaken by a group of terrorists from within one State against critical infrastructure located in another as an armed attack by those cyber terrorists against the latter State"[1109].

---

available at https://www.cfr.org/backgrounder/al-qaeda-aka-al-qaida-al-qaida, {visited on 17 September 2017}.

[1106] WRIGHT, L., "The Terror web", *The New Yorker*, 2 August 2004, available at https://www.newyorker.com/magazine/2004/08/02/the-terror-web, {visited on 26 June 2018}.

[1107] MURPHY, J. F., "Cyber war and International Law…", *op. cit.*, p. 337.

[1108] See ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 11; BRING, O., "The use of force under the UN Charter: modification and reform through practice or consensus", in EBBESSON, J., *et al.* (eds.), *International law and changing perceptions of security: liber amicorum Said Mahmoudi*, Nijhoff, 2014, p, 1-13, at p. 4-6; ROSCINI, M., *Cyber operations…, op. cit.*, p. 84; and *Tallinn Manual 2.0, op. cit.,* rule 71, par. 17.

[1109] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 19.

Then, in light of *Tallinn Manual 2.0*, cyber attacks by non-State actors against the critical infrastructure of another State and without the involvement of another State can constitute an armed attack. In this regard, it mentions that "the object of a cyber operation meeting the trans-border and scale and effects requirements may also determine whether it qualifies as an armed attack. If it consists of property or persons within the affected State's territory, whether governmental or private, the action is an armed attack against that State"[1110]. Therefore, a cyber operation by an individual with the same scale and effect level of an armed attack by a State can constitute an armed attack. However, there is no consensus among experts of *Tallinn Manual 2.0*. While some scholars assert that those attacks, purely motivated by private interests, would not constitute an armed attack to justify the right of self-defence, others are indifferent to their motivations[1111].

As has been observed, according to the unwilling or unable standard, even if the attacks of non-State actors are not attributed to the territorial State, in *extreme situations* a victim State is authorized to use the force in the right of self-defence against such actors. That is why, if a host State cannot control its territory to repel armed attacks by non-State actors, a victim State, based on the requirement of necessity, has the justification to respond in the right of self-defence directly and exclusively against non-State actors to avert such attack[1112].

To justify the right of self-defence, at first, a victim State must require the territorial State to end the attack and give an opportunity to address the situation[1113] or, alternatively, authorize it to act. As a result, the right of self-defence is accepted if its request is fruitless and, thus, its immediate reaction is necessary[1114] (in extreme situations).

[1110] *Ibid,* rule 71, par. 21.

[1111] *Ibid.*

[1112] KREß, C., "Some reflections on the international legal framework governing transnational armed conflict", *JCSL*, 15, 2010, p. 245-274, at p. 250; see also *Tallinn Manual, op. cit.*, rule. 33, par. 3.

[1113] *Tallinn Manual 2.0, op. cit.,* rule 71, par. 26

[1114] DEEKS, A. S., "Unwilling or unable…", *op. cit.*, p. 521-525.

In the field of cyber operations, the host State should seek to ensure that its territory is not used by Non-State actors against other States[1115]. Therefore, to prevent attacks by non-State actors to other States from the very territory of the host State, some measures must be taken. Among others, disable the internet access of the perpetrator; update its firewall settings to prevent hackers from accessing computers under attacks and investigate or arrest those responsible for conducting these attacks against other States[1116]. Although such host State has not developed the necessary technology or ability to repel such cyber attacks, which are qualified as armed attacks, it has the duty to cooperate with the victim State[1117] or rather to authorize the victim State to react against activities of non-State actors. Nevertheless, while it may sound reasonable, it is not easy[1118].

If a host State is unable to prevent such attacks by non-state actors, either because it does not have financial or technical resource to get over the threat[1119] or because it is unwilling to act against such non-State actors, response in the right of self-defence can only be justified in the case of a specific and extreme situation[1120]. However, considering the unwilling or unable standard, the amount of time provided to the host State to respond must be assessed in good faith in relation to the imminence and graveness of the threat[1121].

[1115] UNGA, Doc. A/70/174 "Group of governmental experts…", op. cit., par. 28(e).

[1116] See ROSCINI, M., *Cyber operations…, op. cit*., p. 85-86; SKLEROV, M. J., "Solving the dilemma of State responses to cyber attacks: a justification for the use of active defenses against States who neglect their duty to prevent", *Military Law Review,* 201, 2009, p. 1-103, at p. 62; BRUNNEE, J.; MESHEL, T., "Teaching an old law new tricks: International Environmental law lessons for cyberspace governance", G*YIL,* 58, 2015, p. 129-168, at p. 144-146; see also COE, *International and Multi-stakeholder co-operation on cross-border internet*, interim report of the Ad-hoc Advisory Group on Cross-border Internet to the steering Committee on the Media and New Communication Services incorporating analysis of proposal for international and multi-stakeholder co-operation on cross-border Internet, H/Inf, 2010, par. 21, available at http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf, {visited on 12 June 2018}.

[1117] ROSCINI, M., *Cyber operations…, op. cit*., p. 86, in this regard host State obliges to cooperate "with the victim-State of cyber attacks that originated from within their border" during their investigation and prosecutions.

[1118] "prioritization of consent and cooperation", see DEEKS, A. S., "'Unwilling or unable'…", *op. cit*., p. 519;

[1119] TRAPP. K. N., *State responsibility for international terrorism*, OUP, 2011, p. 71.

[1120] RUYS, T., *'Armed attack'…, op. cit.,* p. 496.

[1121] ROSCINI, M., *Cyber operations…, op. cit*., p. 86; see also DEEKS, A. S., "Unwilling or unable…", *op. cit*., p. 525.

The application of the unwilling and unable standard in the field of cyber attacks finds its support in the legal literature[1122]. In this regard, the US DoD declares that

> "the International Law of self-defence would not generally justify acts of 'active defence' across international boundaries unless the provocation could be attributed to an agent of the nation concerned, *or* until the sanctuary nation has been put on notice and given the opportunity to put a stop such private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile"[1123],

In relation to cyber operations, it also asserts that

> "Adheres to well-established processes for determining whether a third country is aware of malicious cyber activity originating from within its borders. In doing so, DoD works closely with its interagency and international partners to determine: {…} the ability and willingness of a third country to respond effectively to the malicious cyber activity; and the appropriate course of action for the US government to address potential issue of third-party sovereignty depending upon the particular circumstances"[1124].

As a result, according to the US DoD, the inability and unwillingness of the host State to take effective measures to repel the malicious cyber activity from its territory can justify the right of self-defence against non-State actors.

[1122] See HOLLIS, D. B., "Why States…", *op. cit.*, p. 1050; ROSCINI., *Cyber operations…, op. cit*., p. 86; also this is the view of the majority of legal experts in *Tallinn Manual 2.0…, op. cit.,* rule 71, par. 25.

[1123] US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment…, op. cit*, May 1999, p. 22-23 (italic is ours).

[1124] US, DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT, *A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, November 2011, p. 8, *op. cit*.

In this context, the principle of due diligence requires States to take all feasible measures to end cyber operations by non-State actors that are originated in its territory[1125]. Nevertheless, it seems there is not a specific settlement on the precise scope of action required by the *due diligence principle*[1126]. In this sense, although "the unwilling/unable standard is one of the due diligence", regarding the nature of cyber space, "strict liability would be an unacceptable high burden on States, considering to difficulty of preventing cyber intrusions and the ease with which computers can be remotely controlled and identities spoofed"[1127]; for instance, the US has a very large cyber infrastructure and may not be able to detect which of their own servers are being used by hackers to conduct cyber activities against other States[1128]. Also, in practice, a precise delimitation between permissible communication over the internet and impermissible use of cyber infrastructure for military purposes would be difficult[1129]. However, we must keep in mind that in the cyber space context, the *unwilling standard* can open the doors to abuses which can be contrary to the exceptional conception of the right of self-defence.

Regarding the right of self-defence against cyber operations by non-State actors, it is important to point out that International Law only regulates such operations by non-State actors in limited cases[1130]. In order for a cyber attack to constitute an armed attack, the purpose of such attack by a non-State actor must be against political or national security of another State to violate its sovereignty[1131]. In other words, those cyber operations without political or national security purposes can be generally understood as individual

---

[1125] *Tallinn Manual 2.0, op. cit.,* rule 7; UNGA, Doc. A/70/174 on "Group of Governmental Experts…", op. cit., par. 13(h).

[1126] *Ibid*, rule 7, par. 1

[1127] ROSCINI, M., *Cyber operation…, op. cit*., p. 87; in this context some scholars assert that "a certain lack of economic and technological capacity of a particular State might reduce its due diligence obligations" NEY, M.; ZIMMERMANN, A., "Cyber security beyond the military perspective: International Law, 'cyberspace' and the concept of due diligence", *GYIL*, 58, 2015, p. 63; see also KOLB, R., "Reflections on due diligence duties and cyberspace", *GYIL,* 58, 2015, p. 123.

[1128] DÖRR, O., "Obligation of the State of origin of a cyber security incident", *GYIL*, 58, 2015, p. 87-99, at p. 95.

[1129] REINISCH, A.; BEHAM, M., "Mitigating risks: inter-State due diligence obligations in case of harmful cyber incidents and malicious cyber activity-obligations of the transit State", *GYIL*, 58, 2015, p.101-112, at p. 109.

[1130] *Tallinn Manual 2.0, op. cit*., rule 33.

[1131] *Ibid,* rule 33, par. 2.

cybercrimes[1132]; for instance, the action of Kremlin kids, private hackers who allegedly shut down Georgian internet during the Russian invasion of South Ossetia[1133].

In fact, cybercrime encompasses a broad range of illegal activities which are fraudulent practices on the internet, online piracy, storage and sharing of child pornography on a computer and computer intrusions. In this sense, all internet fraud, identity theft and intellectual property piracy by non-State actors are cybercrimes[1134]. However, cybercrime is generally criminalized under domestic law and, in certain cases, International Law[1135].

As a result, in the fields of cyber attacks by non-State actors, such cyber attacks with enough scale and effects can constitute an armed attack even if such attack is not attributed to a State. In extreme circumstances and based on the necessity criteria, a victim State, according to the *unwilling and unable standard*, is allowed resort to the right of self-defence to target non-State actors located within the territory of another State where cyber operations occur for political or national security purposes. However, regarding the nature of cyber attacks, assessing the willingness or unwillingness of a host State is a very difficult task.

[1132] "Cyber-crime is generally understood as the use of a computer-based means to commit an illegal act", HATHAWAY, O. A., *et al*., "The law of cyber-attack", *op. cit.,* p.834; see also GORDON, S.; RICHARD, F., "On the definition and classification of cybercrime", *Journal in Computer Virology,* 2(1), 2006, p. 13-20, at p. 13; and BRENNER, S. W., "Cybercrime, cyber terrorism and cyber warfare", *Revue Internationale de Droit Penal,* 77(3), 2006, p. 453-471, at p. 454. Moreover, the Council of Europe Convention on Cybercrime, covers a broad range of criminal activity committed by means of a computer, including "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data"; *Tallinn Manual 2.0, op. cit*., rule 33, par. 2.

[1133] SHACHTMAN, N., "Kremlin kids: we launched the Estonian cyber war", 11 March, 2009, available at https://www.wired.com/2009/03/pro-kremlin-gro/, {visited 20 April 2018}; and HATHAWAY, O. A., *et al*., "The law of cyber-attack", *op. cit*., p. 831; see also VENTRE, D., *Information warfare, op. cit.,* p. 195.

[1134] HATHAWAY, O. A., *et al*., "The law of cyber-attack", *op. cit*., p. 830.

[1135] *Ibid*, p. 834.

3. The attribution of the cyber attacks

In this part, at first, we are going to cope with the problem of the attribution of cyber operations to the State. Second, we will examine International Law's criteria on the direct attribution to a State of attacks unleashed by its organs. And third, we will analyse International Law's criteria on the indirect attribution to States of attacks by non-State actors, that attack may act on the instructions or under direction or control of a State. In fact, the attribution assists to ensuring that States do not target innocent people or places[1136].

a) *The problem of the attribution of the cyber attacks*

The term attribution is used to identify the party whose responsibility should be assigned for the cyber operation that harms the target interests. The attribution is necessary to identify the entity responsible and involved in the operation[1137]. In other words, attribution is defined "as determining the identity or location of an attacker or an attacker intermediary"[1138].

One of the major challenges to use of the right of self-defence against a cyber attack has been the problem of attributing or determining where an attack came from and who was engaged in it[1139]. This problem gets worse when most of the attacks have occurred by non-State actors rather than States; in this situation, it is more difficult to identify the attackers. Regarding the attribution and the role of non-State actors in cyber attacks, Koh affirms that

---

[1136] CONDRON, S. M., "Getting it right: protecting American critical infrastructure in cyber space", *Harvard Journal of Law and Technology*, 20(2), 2006-2007, p. 403-422, at p. 414; and HOISINGTON, M., "Cyberwarfare…", *op .cit*., p. 451.

[1137] CLARK, D. D.; LANDAU, S. "Untangling attribution", in NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, *Proceedings of a workshop on deterring cyber attacks. Informing strategies and developing options for U.S. Policy*, The National Academies Press, 2010, p. 25-40 at p. 31-32; and, LIN. H., "Escalation dynamics and conflict termination in cyberspace", *Strategic Studies Quarterly*, 6(3), 2012, p. 46-70, at p. 69.

[1138] WHEELER, D. A., *et al*., "*Techniques for cyber attack attribution"*, *Institute for Defense Analyses, (No. IDA-P-3792),* October 2003, p. 1.

[1139] MURPHY, J. F., "Cyber war…", *op. cit*., p. 337.

"cyberspace significantly increases an actor's ability to engage in attacks with 'plausible deniability", by acting through proxies[1140].

In the field of cyber operations, one of the reasons which legal scholars mostly disagree about when applying *ius ad bellum* standard to cyberspace threat is the difficulty to attribute cyber attack directly or conclusively to a specific State[1141]. Indeed, the identification of who carried out cyber operations is a complex problem that basically, in practice, undermines the theoretical entitlement of a State to exercise the right of self-defence[1142].

Attribution is a very critical and complicated issue in the case of cyber attacks because of the technical nature of the cyber domain[1143]. In this regard, three particular characteristics of cyber space make it extremely difficult to attribute cyber operation to a State: i) *anonymity*, ii) *multi-stage cyber attacks*, and iii) *speed at which the cyber attack can be materialized*[1144].

First, *anonymity* is one of the fundamental challenges to notice the attribution when everybody can hide the origin of cyber attacks by tricking it, such as IP spoofing and the use of botnets[1145]. In this sense, the US DoD states that the originator of the attack is great problem "especially when the intruder has used a number of intermediate relay points, when he has used an 'anonymous bulletin board' whose function is to strip away all information about the origin of messages it relays, or when he has used a device that generates false origin information"[1146]. In the same direction, Graham affirms that

[1140] KOH, H. H., "International Law…", *op. cit.*, p. 8.

[1141] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit.*, p. 120.

[1142] DINSTEIN, Y., "Computer network attacks…", *op. cit.*, p. 111.

[1143] MICHAEL, B.; WINGFIELD, Th., "International legal reform could make States liable for cyber abuse, *Journal of European Security and Defense Issue*, 2(2), 2011, 40-41.

[1144] TSAGOURIAS, N., "Cyber attacks…", *op. cit.*, p. 233.

[1145] DELIBASIS, D., *The right to national self-defense in information warfare operations*, , Arena, 2007, p. 303.

[1146] US DoD, *An assessment…, op. cit.,* p. 21.

> "Given anonymity of the technology involved, attribution of a cyber attack to a specific State may be very difficult. While a victim State might ultimately succeed in tracing a cyber attack to a specific server in another State, this can be an exceptionally time-consuming process, and even then, it may be impossible to definitely identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used these as 'zombies' in conducting attacks"[1147].

Hence, to the standpoint of Graham, anonymity characteristics of cyber operations are a great challenge to attribute cyber attack to a specific State or at least it is a time-consuming process.

Second, the most challenging and complex characters of cyber attacks is when there is the possibility of launching *multi-stage cyber attacks* in cyber space where a considerable number of computers operate by different people located in different jurisdictions[1148]. When cyber attack originates from a specific State, it does not necessarily mean that the host State has been involved or is behind such attack[1149]. Moreover, "the nature of digital information infrastructure facilities anonymity, and adversaries can route their attacks through others' computer systems"[1150]. For instance, a cyber attack such as *Solar Sunrise* in 1998, which broke the US DoD's system, was carried out by an Israeli teenager and Californian students through a computer based in the United Arab Emirates[1151].

And third, one of the problems in the field of cyber space is the identification of the attackers that represent a challenge to substantiate the cyber attack, where the *speed* of such attack process and the use of tricky ways that hide the origin make it difficult to

---

[1147] GRAHAM, D. E., "Cyber Threats and the Law of War", *Journal of National Security Law & Policy*, 4, 2010, p. 87-96, at p. 92; see also JENSEN, E.T., "Computer attacks…", *op. cit*., 232.

[1148] CLARK, D. D.; LANDAU, S. "Untangling attribution…", *op. cit*., p. 27.

[1149] BRENNER, S. W., "'At light speed'…", *op. cit*., p. 424; ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 12.

[1150] WAXMAN, M. C., "Cyber–attacks and use of force…", *op. cit*., p. 443-444.

[1151] SHACKELFORD, S. J., "From Nuclear war to net war: analogizing cyber tacks in International Law", *Berkeley Journal of International Law*, 27(1), 2009, p. 192-252, at p. 204 and 231.

identify who and where the cyber attack was being conducted from. Thus, the speed at which the cyber attack can be materialized is another feature that brings about difficulties to the identification of the real mastermind behind such attacks, especially when it is done in a timely and accurately manner[1152]. For instance, the DDoS attacks to Estonia in 2007 involved a large *botnet* of approximately 85.000 hijacked computers from more than 178 countries[1153], which made it difficult to find the real coordinators or, in other words, track down the real mastermind behind the attack.

Even if science is under continuous development, the attribution mechanism to trace back the machine to where the attack was first launched in an era where cyber attacks can be launched even easier by groups or individuals, the identification of the attacker can never be conclusive[1154]. Recent developments in computer technology have made it easier to identify the source of cyber attacks[1155] but "at the same time anti attribution mechanism are also developing which can hide the provenance of the attack"[1156]; Such systems, such as *Tor*, are being used by the military to anonymize their users.

Moreover, "even, if individual perpetrator can be identified, it is so difficult to substantiate as a matter of fact on whose behalf they are operating"[1157]. Then, on the one side, the lack of basis to clarify 'sufficient attribution' and, on the other side, the technological complexities to notice the attacker, led by actors (non-State actors and States) without fear of being caught, convicted and punished for using cyber operations against other States[1158].

[1152] CLARK, D. D.; LANDAU, S. "Untangling attribution", *op. cit*., p. 37.

[1153] TIKK, E., *et al., International cyber incidents…, op. cit.,* p. 20 and 23.

[1154] BOEBERT, E., "A survey of challenges in attribution", in NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, *Proceedings of a workshop on deterring cyber attacks. Informing strategies and developing options for U.S. Policy*, The National Academies Press, 2010, p. 43-48, at p. 41-55.

[1155] DINSTEIN, Y., "Computer Network attacks…", *op. cit*., p. 112.

[1156] TSAGOURIAS, N., "Cyber attacks…", *op. cit*., p. 234.

[1157] WAXMAN, M. C., "Cyber–attacks and use of force…", *op. cit*., p. 444.

[1158] HUNKER, J., *et al*., "Role and challenges for sufficient cyber-attack attribution", *Institute for Information Infrastructure Protection*, 2008, p. 4-5.

Furthermore, these technical issues are exacerbated by the jurisdiction concerns when States have limitations to investigate beyond their borders, especially when electronic attacks can include transit computers and networks spanning dozens of countries[1159]. Also, even if the investigation process can pursue a cyber attack through digital networks, there are difficulties to publish that information in a timely and convincing way, particularly when States do not have the motivation to discuss about technical details of information security to reveal their capabilities to adversaries or third parties[1160]. Also, tracing cyber attacks back can be an exceptionally prolonged process, and "identify the entity or individual directing the attack is extremely hard"[1161].

As a result, achieving direct and concessive attribution to cyber attacks is not easy[1162]. This fact makes it complex to use legal enforcement measures, when attribution must be clear with *convincing evidence*. Hence, some scholars proposed to use a transnational criminal approach and to establish international jurisdiction to investigate an prosecute individuals or groups under domestic and International Law[1163].

b) *International Law criteria on direct attribution: evidentiary issue*

In general, in order to attribute an armed attack to a State, there are two main situations: the first and easiest scenario is *de jure organs* of a State, when the cyber attack occurs with *uniformed* hackers[1164]; and second, *de facto organs,* that includes those individuals' attacks which are attributed to a State because they are instructed, directed, controlled by such State.

[1159] WAXMAN, M. C., "Cyber–attacks and use of force…", *op. cit*., p. 444; in this context, Koh affirms that "because of the interconnected, interoperable nature of cyber space, operations targeting networked information infrastructure in one county may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered", KOH, H. H., "International Law…", *op. cit*., p. 6.

[1160] WAXMAN, M. C., "Cyber–attacks and use of force…", *op. cit*., p. 444.

[1161] JENSEN, E.T., "Computer attacks…", p. 207.

[1162] HADJI-JANEV, M., "Information legal aspects of protecting civilians and their property in the future cyber conflict", in INFORMATION RESOURCES MANAGEMENT ASSOCIATION (ed.), *Cyber security and threats: concept, methodologies, tools, and applications*, IGI Global, 2018, p. 1555-1583, at p. 1567.

[1163] MICHAEL, B.; WINGFIELD, Th., "International legal…", *op. cit*., p. 41.

[1164] ROSCINI, M., *Cyber operations*…, *op. cit*., p. 34.

In relation to the first scenario, the victim State of an armed attack is authorized to use the right of self-defence if it meets International Law's attribution standard to *de jure* organs of one State[1165]. In this sense, article 4 of *Draft Articles on the Responsibility of States for International Wrongful Acts* provides that

> *"*The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State {and}, An organ includes any person or entity which has that status in accordance with the internal law of the State"[1166].

Then, any cyber activity by the organ of a State can be considered an act of such State no matter whether such organ is under the control of the central government or another territorial unit of the State. In other words, *de jure* organs of a State "covers all the individual or collective entities which make up the organization of the State and act on its behalf. It includes an organ of any territorial governmental entity within the State on the same basis as the central governmental organs of that State"[1167]. It means that the concept of State organs is not limited to the organs of the central government and it can be extended to a governmental of any kind or classification, exercising any functions at any level in the hierarchy, even at the local level[1168]. In the field of cyber operation, this approach is reaffirmed by *Tallinn Manual 2.0* that

> "The concept of 'organs of a State' in the law of State responsibility is broad. All persons or entities that have that status under the State's domestic laws are State organs regardless of their function or place in the governmental hierarchy. Thus, any cyber activity undertaken by the intelligence, military,

[1165] TSAGOURIAS, N., "Cyber attacks…", *op. cit*., p. 236

[1166] ILC, "Draft articles on Responsibility of States...", *op. cit.,* vol. ll, part 2, 2001, article 4.

[1167] *Ibid*, article 4, commentary (1).

[1168] *Ibid*, article 4, commentary (6).

> internal security, customs, or other State agencies engages State responsibility if it violates an international legal obligation binding on that State"[1169].

As a result, there is a broad view in the concept of *de jure* organs when it includes any person or entity which has that status in conformity with the internal law of the State.

Thus, if *de jure* organs of a State commit a cyber attack, this will be directly attributed to such State and the victim State will be authorized to exercise the right of self-defence[1170]. In this sense, we must point out that recently many States have established cyber units to conduct cyber operations; for instance, China has created cyberspace battalions and regiments[1171]; Israel declares that its soldiers are working on an "internet warfare team"[1172]. Also, the US established a military cyber command to confront cyber attacks[1173]. In Spain, there is the *Centro Criptológico Nacional-Computer Emergency Response Team* (CCN-CERT), which has the capacity to respond to information first security incidents of the National Cryptological Center, created in 2006 as the CERT. Also, the Joint Command of Cyberdefence of the Armed Forces was established in 2013[1174]. Hence, cyber attacks by these units would be imputed to the State of which they are *de jure organs.*

However, to resort to the right of self-defence against another State, the victim State must provide appropriate *evidence* to substantiate an armed attack to such State. In the field of the attribution, evidence is defined as "required to prove both the objective (be it an act or

---

[1169] *Tallinn Manual 2.0, op. cit.*, rule 15, par. 2.

[1170] TSAGOURIAS, N., "Cyber attacks…", *op. cit.*, p. 236.

[1171] CONDRON, S. M., "Getting it right…", *op. cit.*, p. 405; and ROSCINI, M., "World wide warfare …", *op. cit.*, p. 97-98.

[1172] CHRISTIAN, "Israel adds Cyber-attack to IDF", 10 February 2010, available at https://www.military.com/defensetech/2010/02/11/israel-adds-cyber-attack-to-idf, {visited on 22 May 2018}.

[1173] US, DoD, *Cyber Strategy*, 17 April 2015, p. 13, available at https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, [visited on June 2018].

[1174] See DOMINGUEZ, J., "La ciberseguridad: aspectos juridicos internacionales", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2014*, Aranzadi, 2015, p. 161-223, at p. 169-178.

an omission) and subjective elements of an internationally wrongful act"[1175]. The International Law does not determine specific evidentiary standards to clarify wrongful acts as the originator of an armed attack[1176]. Nevertheless, it is required that any State, in order to justify the right of self-defence against another State or non-State actors, provide enough evidence.

The ICJ in the *Nicaragua case* declared that "within the limit of its status and rules {...} {the Court} has freedom in estimating the value of the various elements of evidence"[1177], but avoided to clarify the standards of evidence. Effectively, the Court, in its primary judgment in the *Corfu Channel*, referred to "conclusive evidence" or "a degree of certainty" and in relation to wether Albania had acknowledged the minelaying in her territorial waters, it pointed out that "the proof may be drawn from inferences of fact, provided that they leave *no room* for reasonable doubt"[1178]. Also, this approach was pursued by the ICJ in the *Nicaragua case*[1179], *Oil platforms*[1180] or the *Legality of armed activities in the territory of Congo*[1181].

A similar formula is explicitly expressed in the US notification in 2001 to the UNSC to justify the right of self-defence, where the US officially declared that "my government has obtained *clear and compelling* information that the *Al-Qaeda* organization, which is supported by the

[1175] ROSCINI, M., *Cyber operation…, op. cit*., p. 97-98.

[1176] SCHMITT, M. N., "Cyber operations…", *op. cit*., p. 168.

[1177] ICJ, *Nicaragua case, op. cit*., par. 60.

[1178] ICJ, *Corfu Channel case , op. cit.,* p. 18; see GREEN, J. A., "Fluctuating evidentiary standards for self-defence in the International Court of Justice", *International & Comparative Law Quarterly*, 58(1), 2009, p.163-179, at p. 172; and ROSCINI, M., *Cyber operations…, op. cit*., p. 99.

[1179] The ICJ in *Nicaragua case* by referring to "convincing evidence" (par. 29), it emphasized that "Yet despite the heavy subsidies and other support provided to them by the United States, there is no clear evidence of the United States having actually exercised such a degree of control in all fields as to justify treating the *contras* as acting on its behalf", ICJ, *Nicaragua case, op. cit*., par. 109.

[1180] The ICJ mentioned that there is "highly suggestive, but not conclusive" to accepting Iranian responsibility for minelaying, see ICJ, *Oil platform case, op. cit*., par. 71.

[1181] The ICJ referred to "convincingly established by the evidence", "convincing evidence", see ICJ, *Legality of armed activities in territory of Congo, op. cit*., pars, 72, 91 and 136.

Taliban regime in Afghanistan, had a central role in the attack"[1182]. Additionally, the same language is used by NATO Secretary-General[1183]. Furthermore, in reaction to the proposal of military intervention against Syria Government that was accused of using chemical weapons, the US President asserted that any military activities against another State without the UN mandate or "clear evidence that can be presented" is not lawful[1184]. Finally, the Dutch *Advisory Council on International Affairs* requires "reliable intelligence {...} before a military response can be made to a cyber attack" and "sufficient certainty" about the identity of the authors of the attack[1185]. In this regard, it seems that State practice indicates that, based on clear and convincing evidence, States can substantiate attacks to others in self-defence[1186].

In relation to the nature of cyber space, most of cyber attacks are not clear and the access to conclusive evidence to prove who conducts a cyber attack is very difficult; for instance, in the cyber attack in Georgia, *NATO Cooperative Cyber Defense Center of Excellence* (CCDCOE) mentioned that "there is no conclusive proof of who is behind the DDoS attack, although fingers pointing at Russia is prevalent by the media"[1187]. This led to raising the question of whether it is possible to decrease the standard of evidence that is required for the exercise of the right of self-defence in the context of cyber attacks.

In favour of decreasing the standard of evidence, the US declares that "the identity and motivation of the perpetrator(s) can only be inferred from the target, effects and other

---

[1182] Letter dated on 7 October 2001 from the Permanent Representative of the US to the UN addressed to the President of the UNSC, UN Doc. S/2001/946, 7 October 2001 (italic is ours).

[1183] "The facts are clear and compelling. The information presented points conclusively to an Al-Qaida role in the 11 September attacks", Statement at NATO Headquarters, 2 October 2001, available at https://www.nato.int/docu/speech/2001/s011002a.htm, {visited on 15 March 2018}.

[1184] BORGER, J., "West reviews legal options for possible Syria intervention without UN mandate", *The Guardian*, of 26 August 2013, available at https://www.theguardian.com/world/2013/aug/26/united-nations-mandate-airstrikes-syria {visited on 2 April 2018}.

[1185] DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*…, *op. cit*., p. 22.

[1186] O'CONNELL, M., E., *et al*., "Cyber security…", *op. cit*., p. 7.

[1187] TIKK, E., *et al*., *Cyber attacks against Georgia: legal lessons identified*, CCDCOE, November 2008, p. 1-45,at p. 12, available at http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf,]visite don 2 March 2018[.

circumstantial evidence surrounding an incident"[1188]. Similarly, the US DoD *An Assessment of International Legal Issues in Information Operation* asserts that "State sponsorship might be persuasively established by such factors as signals or human intelligence, the location of the offending computer within a State-controlled facility, or public statements by officials", and that "the State of relationship between the two countries, prior involvement of the suspect State in computer network attacks, the nature of systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks"[1189]. Then, in accordance with the US view, the identification and attribution are a problematic issue in the digital environment and to overcome this problem it suggests a standard of proof lower than a clear and convincing evidence. However, this approach is far from being unanimous in the international community[1190], even within the US Departments[1191].

Therefore, the clear and convincing evidence obliges a State to act reasonably is an appropriate standard to claim the right of self-defence against all kind of traditional armed attacks and cyber operations[1192]. In this sense, Schmitt asserts that *clear* and *convincing* evidence, in essence, obliges a State to act reasonably and does not authorize States to

[1188] UNGA, Doc. A/66/152 on "Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General", 15 July 2011, p. 16-17.

[1189] US, DoD, *An Assessment…, op.cit*., p. 21

[1190] For instance, Germany referred to "reliable attribution" of malicious cyber activities in order to prevent "false flag" attacks, misunderstanding and miscalculations, see *Permanent Mission of the Federal Republic of Germany to the UN*, Note verbale No 516/2012, 5 November 2012; or the *AIV/CAVV report* where the Dutch Government refers to "reliable intelligence {…} before a military response can be made to a cyber attack", DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*…, *op. cit*., p. 22.

[1191] For example, attribution of cyber operations should be conduct with "sufficient confidence and verifiability", see US AIR FORCE, *Cyber Operations. Air Force Doctrine Document 3-12*, 15 July 2010, p. 10. available at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-060.pdf, [visited on 10 March 2018].

[1192] OHLIN, J. D., *et al.* (eds.), *Cyber war: law and ethics for virtual conflicts*, OUP, 2015, p. 230-231; ROSCINI, M., *Cyber operation…, op. cit*., p. 102; see also O'CONNELL, M. E., "Rules of evidence for the use of force in International Law's new era", *Proceedings of the Annual Meeting (American Society of International Law),* 100, 2006, p. 39-54, at p. 45.

respond in the right of self-defence rapidly on the basis of sketchy indications of who has attacked until it gathers unassailable evidence[1193].

As a result, in order to invoke the right of self-defence, it seems that "clear or convincing evidence" is necessary[1194], because this right is an exception to the prohibition of the use of force, and the standard of evidence must be high enough to limit and prevent the abuse of such right[1195].

Then, "the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure {...}, is usually insufficient evidence for attributing the operation to that State"[1196]. Thus, when a victim State has taken reasonable steps or rational conclusions to attribute an armed attack to the perpetrator of the cyber or kinetic attack, it may react in the right of self-defence; also, this reasonable standard must be applied in anticipatory self-defence when cyber attack is imminent[1197].

In addition, to impute an armed attack to a State, the political climate where the attack took place or who benefited from the attack must be also taken into consideration[1198]; hence, accounting the motivation of the State to conduct an attack can be functional to substantiate the cyber attack. Nevertheless, motivation alone is not enough reasonable evidence to impute an attack to a State. In other words, States cannot recourse to the right of self-defence based on casual evidence or wild political inferences[1199].

[1193] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 168.

[1194] O'CONNELL, M. E., "Evidence of terror", *JCSL*, 7(1), 2002, p. 19-36, at p. 22.

[1195] ROSCINI, M., *Cyber operations*…, *op. cit.*, p. 99.

[1196] *Tallinn Manual 2.0, op. cit.,* rule 15, p. 13; see also UNGA, Doc. A/70/174 "Group of Governmental Experts …", *op. cit.*, par. 28(f); and REINISCH, A.; BEHAM, M., "Mitigating risks: inter-State …", *op. cit.*, p. 110.

[1197] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 168.

[1198] TSAGOURIAS, N., "Cyber attacks…", *op. cit.*, p. 234.

[1199] *Ibid*, p. 235.

c) *International Law criteria on indirect attribution: special reference to effective control*

According to ILC, "as a general principle, the conduct of private persons or entities is not attributable to the State under International Law {however, when} there exists a specific factual relationship between the person or entity engaging in the conduct and the State", to attribute such conduct to the State[1200]. Then, State can also be responsible for attacks that are indirectly attributed to its *de facto* organs.

In this regard, any attack by entities instructed, directed or controlled by a State can be attributed to that State[1201]. According to ILC, *de facto* organs, on one side, include entities empowered by authorities of the State that are assimilated to or are absorbed in the State apparatus (article 5) and, on the other side, include entities which are acting according to the instructions of, or under the direction or control of, that State (article 8)[1202].

In relation to the persons or entities empowered by a State, article 5 of *Draft Articles on Responsibility of States* provides that

> "the conduct of a person or entity which is not an organ of the State under article 4 {*de jure* organs} but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance" (article 5).

Then, this situation is limited to entities which are empowered by internal law to exercise governmental authority and are distinguished from situations where entities are under the direction and control of States[1203]. In the context of cyber operation, *Tallinn Manual 2.0*

[1200] ILC, "Draft Articles on Responsibility of States…", *op. cit*, vol. ll, part 2, 2001, article 8, commentary (1); see also *Tallinn Manual 2.0, op. cit.,* rule 17, par. 1; UNGA, Doc. A/70/174 on "Group of Governmental Experts…", *op. cit*., par. 28 (e).

[1201] *Tallinn Manual 2.0, op. cit.,* rule 17(a).

[1202] ILC, "Draft Articles on Responsibility of States…", *op. cit*, vol. ll, part 2, 2001.

[1203] *Ibid*, article 5, commentary (7).

affirms that "cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State"[1204].

In this respect, *persons or entities* reflect a wide variety of bodies that may be empowered by the law of the State to exercise elements of governmental authority that may include public corporations, semi-public entities, public agencies and even, in particular cases, private companies[1205].

In the context of cyber attacks, hackers can be members of parastatal entities, or public, semi-public or privatized corporations empowered by domestic law to exercise some degree of governmental authority[1206]. Although hackers are individuals and are not *de jure organs* of the State, if they are hired by the State to conduct cyber attacks, such attacks can be attributed to that State. A very well-known example in this field is the *Russian Business Network* (RBN), a firm specialized in phishing, DDoS attack, etc., that executed cyber attacks against Georgia on behalf of Russia.

In fact, attributing the attack to military or organs of a State would not change norms when the hackers are civilians and are not uniformed organs[1207]. This approach is implied in the ICJ's view where armed attacks can be carried out by all groups or bands on behalf of one State against another State where the first State is substantially involved therein[1208].

[1204] *Tallinn Manual 2.0, op. cit.,* rule 15.

[1205] *Ibid*, article 5, commentary (2).

[1206] ROSCINI, M., *Cyber operations…*, *op. cit.*, p. 35.

[1207] *Ibid*, p. 34.

[1208] ICJ, *Nicaragua case, op. cit*., par. 195.

Nowadays, it seems that States prefer using cyber technology by its State agents to conduct cyber attack because it is a perfect tool to carry out its hostile and covert measures with little public acknowledgment[1209]. In this sense, *Tallinn Manual 2.0* proclaims that

> "in addition to the acts of State organs, acts committed by persons or entities that do not qualify as State organs, but that are empowered by domestic law (e.g., legislation, administrative act, or, if domestic law so provides, by contract) to exercise elements of governmental authority, are attributable to the State"[1210].

Thus, those private corporations that have been granted legal authority by the government or empowered or sponsored by the authorities of State to conduct offensive cyber operations against another State imply State responsibility[1211]. This rule is created to ensure that States do not conceal themselves behind non-State actors or private actors to engage in conducts that are internationally wrongful[1212].

In relation to entities acting on the instructions of, or under the direction or control of, a State according to article 8 of *Draft Articles on Responsibility of States* "the conduct of person or group of persons shall be considered an act of a State under International Law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct"[1213].

In this regard, both the conducts of private persons acting on the instructions of the State, on one side, and an increasingly common situation where those "private persons act under

---

[1209] MAHVI, A. J., "Strategic offensive cyber operations: capabilities, limitations, and role of intelligence community, in KOSAL, M. E. (ed.), *Technology and the intelligence community: challenges and advances for the 21st Century*, Springer, 2018, p. 171-182, at p. 174.

[1210] *Tallinn Manual 2.0, op. cit.,* rule 15, par. 8.

[1211] *Ibid*; and KOH, H. H., "International Law…", *op. cit.*, p. 7.

[1212] KOH, H. H., "International Law…", *op. cit.*, p. 7.

[1213] ILC, "Draft Articles on Responsibility of States…", *op. cit.*,, vol. ll, part 2, 2001.

the State's direction or control"[1214], on the other side, can be attributed to that State. In the context of the *direction or control*,

> "such conducts will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation. The principle does not extend to conduct which was only incidentally or peripherally associated with an operation and which escaped from the State's direction or control"[1215].

These situations must be distinguished from cases where private citizens, on their own initiative, carry out cyber operations, such as *hacktivists* or *patriotic hackers*, since the mere encouragement of independent acts of non-State actors, does not meet the ILC standard (article 8)[1216].

The criterion of *control* is a problematic issue because there is an apparent jurisprudential split in the required degree of control to attribute acts from non-State actors to a State. As mentioned *supra*, in order to constitute an armed attack to authorize the exercise of the right of self-defence, the ICJ in *Nicaragua case* declared that

> "United State participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the *contras*, the selection of military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself {…} for the purpose of attributing to the United States the acts committed by the *contrast* in the course of their military or paramilitary operations in Nicaragua"[1217].

Then, the Court has a restrictive approach to attribute an armed attack to a State to justify the right of self-defence. In this regard, the ICJ emphasised that it is necessary that the State

[1214] *Ibid*, article 8, commentary (1).

[1215] *Ibid*, commentary (3).

[1216] *Tallinn Manual 2.0*, *op. cit*., rule 17, par. 8; see also WALTER, Ch., "Obligations of States before, during, and after a cyber security incident", *GYIL*, 58, 2015, p. 67-86, at p. 73.

[1217] ICJ, *Nicaragua case*, *op. cit*., par. 115.

has the "*effective control* of the State military or paramilitary operation in course of which the alleged violations were committed"[1218]. Hence, States are responsible for the acts of non-State actors when they have *effective control* over such acts[1219].

Again, the ICJ in the *Genocide case* pointed out that "it must {…} be shown that this 'effective control' was exercised or that the State instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations"[1220]. In this sense, the ICJ rejected *overall control* as an attribution standard[1221] and reaffirmed that *overall control* test "has the major drawback of boarding the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting on whatever basis, on its behalf"[1222]. For instance, in the context of the effective control criteria, AIV/CAVV asserts that in the response to the events of 11 September 2001, there was not any consideration to *effective control* criteria in *Nicaragua* judgment, when an organized armed group carried out an armed attack without the State control or substantial State influence[1223].

However, the International Criminal Tribunal for the former Yugoslavia (ICTY), in *Tadic case*, asserts that in order to attribute the conduct of an armed military group to a State, it is sufficient that such State "has a role in organizing, coordinating, or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group {…} regardless of any specific instructions by the

[1218] *Ibid*, par. 115 (italic is ours).

[1219] *Ibid*, par. 115; *Tallinn Manual 2.0*, *op. cit.*, rule 17, par. 5-6.

[1220] ICJ, *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, (Bosnia and Herzegovina *v.* Serbia and Montenegro), judgment of 26 February 2007, *ICJ Reports 2007*, par. 400.

[1221] *Ibid*, pars. 402-406.

[1222] *Ibid*, par. 406.

[1223] DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*…, *op. cit.*, p. 21.

controlling State concerning the commission of each of those acts"[1224]. Thus, an *overall control* test is much less restrictive to attribute the conduct of non-State actors to a State[1225], but the required control would go beyond "the mere financing and equipping of such forces and involves also participation in the planning and supervision of military operations"[1226].

Therefore, there are distinctions between *effective control* test in the view of the ICJ and *overall control test* of the ICTY. It seems that, contrary to the *effective control* test that focuses on the control over the act, the *overall control* emphasises on the actor[1227] and focuses more on the general influence that the State may exercise over the group, not on specific activities; in other words, the overall control standard is much less strict[1228]. In this sense, *Tallinn Manual* asserts that "effective control includes both the ability to cause constituent activities of the operation to occur, as well as the ability to order the cessation of those that are underway"[1229].

Regarding the nature of cyber operations and its specific features, some scholars assert that the *effective control* test would be preferable to the *overall control* test[1230] because, on one side, the *effective control test* prevents States from suffering abuse of the right of self-defence and exonerates them from being maliciously accused of every cyber attacks and, on

---

[1224] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIAI (ICTY), APPEALS CHAMBER, *Presocutor v. Tadic*, case No IT-94-1-A, judgment, 15 July 1999, par. 117.

[1225] ROSCINI, M., *Cyber operations*…, *op. cit*, p. 37; see also AIV/CAVV report which declared that ICTY in its judgment "settled on the slightly broader standard of 'over control'", DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*…, *op. cit*., p. 20; and *Tallinn Manual 2.0*, *op. cit*., rule 17, par. 6.

[1226] ICTY, *Prosecutor v. Tadic*, *op. cit*., par. 145; see also ILC, "Draft articles on Responsibility of States…", *op. cit.,* vol. ll, part 2, 2001, article 8, commentary (5).

[1227] Milanović mentioned that "The overall control is not control over the act, but over the actor, an organized and hierarchically structured group, at a general level", MILANOVIĆ, M.,"State responsibility for acts of Non-State actors: a comment on Griebel and Plücken", *LJIL*, 22(2), 2009, p. 307-324, at p. 317.

[1228] ICTY, *Prosecutor v. Tadic*, *op. cit*., par. 131 and 137; Tsagourias affirms that "The ICTY in the *Tadic case* introduced an alternative-lower-threshold", TSAGOURIAS, N., "Cyber attack,…", *op. cit*., p. 238; and SCHMITT asserts that "the ICTY took a more relaxed view of the degree of control necessary, accepting 'overall control' as sufficient", SCHMITT, M. N. "Cyber operations…", *op. cit*., p. 171; see also DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*…, *op. cit*., p. 20; and *Tallinn Manual 2.0, op. cit*., rule 17, par. 6.

[1229] *Tallinn Manual 2.0*, *op. cit*., rule 17, par. 6.

[1230] SHACKELFORD, S., "From nuclear war…", *op. cit*., p. 232; see also RYAN, D. J., *et al*. "International cyber law…", *op. cit*., p. 1187; and TSAGOURIAS, N., "Cyber attack,…", *op. cit*., p. 239-240.

the other side, it is more functional to cover private individuals who are engaged by a State to conduct cyber operation against another State[1231].

Thus, in accordance with the ICJ and some scholars' view in the context of cyber cyber attacks, only those attacks carried out by entities under the *effective control* of the State can be attributed to such State[1232]. As a result, if a State had effective control over cyber attacks, such attacks by non-State actors can be attributed to that State even if this State does not have a *formal* relation with non-State actors. However, the act of supplying hacking tools by the host State, which are subsequently used by a non-State actors group in its own initiative against another State, cannot be attributed to the host State[1233]. Thus, the mere supplying of hacking tools is insufficient to attribute the activity of that group to the host State. Finally, it is important to point out that, regarding the complex nature of cyber operations, the application of this general principle to each case, must be assessed case by case[1234].

Another potential attribution standard is when hackers are neither *de jure* nor *de facto* State organs, but their conduct has been incited by State authorities[1235]. The ICJ in the *Tehran hostages case* held that the initial attack against the US embassy in Tehran was not attributed to Iran but the subsequent endorsement of Iranian authorities by detention of hostages, transformed the occupation into an act of the State[1236].

In this respect, article 11 of the *Draft Articles on State Responsibility of States* affirms that "conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under International Law if and to extent that the State

[1231] ROSCINI, M., Cyber operations…, *op. cit*., p. 38.

[1232] TSAGOURIAS, N., "Cyber attack…", *op. cit*., p. 238.

[1233] *Tallinn Manual 2.0, op. cit.,* rule 17, par. 19.

[1234] ILC, "Draft Articles on Responsibility…", *op. cit.,* Vol. II, part 2, 2001; and *Tallinn Manual 2.0, op. cit.,* rule 17, par. 11.

[1235] ROSCINI, M., *Cybr operations…, op. cit*., p. 39.

[1236] ICJ, *Tehran hostages case*, *op. cit.,* par. 74.

acknowledges and adopts the conduct in question as its own"[1237]. However, this rule "is narrowly applied. Not only are the conditions of 'acknowledgment' and 'adoption' cumulative, but they also require more than mere endorsement or tacit approval of the non-State actor's operation, albeit not express endorsement"[1238]. Therefore, mere expressions of approval to cyber attacks cannot attribute the responsibility of such attack to the State.

In spite of the ICJ's view in *Nicaragua case* that affirms that "logistical support" or "provision of weapons" to non-State actors cannot attribute armed attack to the host State[1239], we cannot confirm that there is a tendency to stretch such norm in relation to attributing responsibility to other States when internationally they use their cyber capabilities to protect non-State actors against counter cyber operations. In this sense, *Tallinn Manual 2.0* asserts that if another State "internationally employing its cyber capabilities to protect the non-State actor against counter-cyber operations so as to facilitate their continuance as acts of that State, the requirements for attribution have been met"[1240].

According to the *effective control* test, those cyber attacks that are originated by a computer located in a certain State without any State involvement, cannot be attributed to such State in the lack of effective control over the attack[1241]. In this sense, the mere breach of the obligation of "not to allow knowingly its territory to be used for acts contrary to the rights

[1237] ILC, "Draft Articles on Responsibility…", *op. cit.,* Vol. II, part 2, 2001.

[1238] *Tallinn Manual 2.0, op. cit.,* rule 17, par. 16; see also ILC, "Draft articles on responsibility…", *op. cit.,* vol. II, part 2, 2001, article 11, commentary (6) and (9).

[1239] ICJ, *Nicaragua case, op. cit.,* par. 195.

[1240] *Tallinn Manual 2.0, op. cit.,* rule 17, par. 16.

[1241] TSAGOURIAS, N., "Cyber attack…", *op. cit.*, p. 242; UNGA, Doc. A/70/174 on "Group of Governmental Experts on developments…", *op. cit.*, par. 28(f).

of other States"[1242], is not reason enough to attribute the cyber attack to the host State to justify the right of self-defence by the victim State[1243].

In fact, under modern International Law, the application of the concept of due diligence came to situations of risk of transboundary harm within cyberspace. In this field, "the application of this principle {due diligence} would mean that all State share a common obligation to ensure that neither their territory, nor hardware and cyber infrastructure situated on their territory or under their effective control, is misused to harm other States or their residents"[1244]. This approach is reaffirmed by the UN GGE[1245] and particularly in *Tallinn Manual 2.0.* where it proclaims that "a State must exercise due diligence in not allowing its territory, or the territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights and produce serious adverse consequences to the other State"[1246].

Thus, the host State has the duty to exercise due diligence and take the necessary and reasonable measures to stop attacks, such as disabling access to internet[1247]. However, deliberate failures by the host State to perform due diligence or unwillingness to take measures to stop attacks by non-State actors that are originated within the territory of the host State, under specific and extreme situations, cannot exclude the right of the victim State to react directly against non-State actors in self-defence[1248].

[1242] ICJ, *Corfu Channel case, op. cit*., p. 22; and *Tallinn Manual…, op. cit*., rule 5, par. 3; UNGA, Doc. A/70/174 on "Group of Governmental Experts…", *op. cit*., par. 13(c).

[1243] *Tallinn Manual 2.0, op. cit*., rule. 17, par. 16; and ILA, *Draft Report on aggression and the use of force,* Committee on the Use of Force, *op. cit*., 2016, p. 12.

[1244] NEY, M.; ZIMMERMANN, A., "Cyber security beyond the military perspective: International Law, 'cyberspace' and the concept of due diligence", *GYIL*, 58, 2015, p. 51-66, at p. 62; see also HERDEGAN, M., "Possible legal framework and regulatory models for cyberspace: due diligence obligations and institutional models for enhanced inter-State cooperation", *GYIL*, 58, 2015, p. 169-185, at p. 178.

[1245] UNGA, Doc. A/68/98 "Group of Governmental Experts…,", *op. cit*., par. 23; UNGA, Doc. A/70/174 "Group of Governmental Experts…", *op. cit*., 13(c), 28(e).

[1246] *Tallinn Manual 2.0*, *op. cit*., rule 6.

[1247] ROSCINI, M., *Cyber operations…, op. cit*., p. 40.

[1248] *Ibid*.

D. **Other requirements to the exercise of the right of self-defence against cyber attacks**

In light of a sophisticated nature of the new threat on cyber space, it is clear today that the traditional rules of the use of force in cyber space will become obsolete in the far future, but at least it is valuable not leaving the issue unanswered and thinking on the adoption of some kind of guidelines to help States to react new threats[1249]. In this sense, according to International Law, when cyber attacks amount to an armed attack, the victim State must meet the requirements of necessity, proportionality and immediacy to react in the right of self-defence[1250]. In this sense, the right of self-defence must be limited to what is necessary to address an imminent or present armed attack and must be proportionate to the threat that is facing[1251].

1. *Necessity and proportionality*

As previously mentioned, the necessity is one of the requirements to justify the use of force in the right of self-defence. *Necessity* means a "forceful action that is necessary to defend against an attack"[1252]. In the context of cyber attacks, *Tallinn Manual 2.0* notes that "a use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate"[1253].

In the context of the necessity requirement, the ICJ in the *Oil Platforms case* did not accept the justification of the right of self-defence by the US, because it did not previously put any effort to resolve the issue diplomatically[1254]. Thus, based on the necessity criteria, in order to justify the right of self-defence, there must be no reasonable option other than force to effectively deter an imminent attack or ongoing attack. Then, in the context of cyber

[1249] CERVELL, M. J., *La legítima defensa…, op. cit*., p. 303-304.

[1250] See *Tallinn Manual 2.0, op. cit.,* rule 72 and 73; or ROSCINI, M., *Cyber operations…, op. cit*., p. 88.

[1251] BETHLEHEM, D., "Self-defense against an imminent or actual armed attack by non-State actors", *AJIL,* 106(4), 2012, p. 769-777, at p. 772.

[1252] AREND, A. C.; BECK, R. J., *International Law…, op. cit.,* 1993, p. 72.

[1253] *Tallinn Manual 2.0, op. cit.,* rule 72.

[1254] ICJ, *Oil Platforms case*, *op. cit*., pars. 43 and 76.

operations, necessity exists in the lack of alternative non-forceful courses to repel the cyber attack[1255].

Therefore, to accomplish the requirement of necessity, first, the forcible reaction must be a mean of last resort; in other words, "all peaceful policy options that have a reasonable chance of achieving a just cause must be exhausted before the use of force is permissible"[1256]. In this sense, if passive cyber defence is adequate to thwart the cyber attack, or there is an opportunity to settle the dispute in a friendly manner via negotiations, then, forceful defensive measures would be disallowed[1257]. The victim State must apply "the least intrusive methods feasible to mitigate a threat"[1258]. In this regard, the forceful actions may be combined with non-forceful measures, such as diplomacy, economic sanctions, or law enforcement[1259]. Moreover, according to article 51 of the UN Charter, the use of force in the right of self-defence would be unnecessary if the UNSC took measures to restore international peace and security[1260].

The second requirement is to ascertain that the cyber attack "is no accident, to verify the genuine identity of the State -or non-State entity- conducting the attack (so as not to jeopardize innocent parties), and to conclude that use of force as a counter-measure is indispensable"[1261]. Then, to fulfil the necessity requirement, the victim State must attribute the attack to a specific source and confirm the existence of *intention* behind such attack[1262].

[1255] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 167.

[1256] ALOYO, E. *The last of last resort*, The Hague Institute for Global Justice, Working Paper 1, July 2014, p. 1; see also SCHMITT, M. N., "Pre-emptive strategies in International Law", *MJIL,* 24(2), 2003, p. 513-548, at p. 530.

[1257] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 167; *Tallinn Manual 2.0, op. cit.,* rule 72, par. 3; and DINSTEIN, Y., "Computer network attacks…", *op. cit.*, p. 109.

[1258] US, *Presidential Policy Directive/PPD-20*, *op. cit*, p. 8.

[1259] See SALINAS, A. M., "Lucha contra terrorismo internacional: no solo del uso de la fuerza pueden vivir los Estados", *REDI*, 68(2), 2016, p. 229-252, at p. 241-244.

[1260] ROSCINI, M., *Cybr operations…, op. cit.*, p. 89.

[1261] DINSTEIN, Y., "Computer network attacks…", *op. cit.*, p. 109.

[1262] CONDRON, S. M., "Getting it right…", *op. cit.*, 413; and HOISINGTON, M., "Cyberwarfare…", *op. cit.*, p. 450.

In any case, the justification of the exercise of the right of self-defence against a cyber attack which is qualified as an armed attack, depends on the necessity in each circumstance, and "is judged from the perspective of the victim State. The determination of necessity must be reasonable in the attendant circumstances"[1263]. In this sense, it is valuable to

> "Consider a case in which one State is conducting cyber armed attacks against another State's cyber infrastructure. The victim State responds with forceful cyber operations of its own to defend itself. Unbeknownst to that State, the attacking State had already decided to ends its attacks. This fact would not render the victim State's defensive cyber operations unnecessary and, therefore, an unlawful use of cyber force in self-defence"[1264].

Nevertheless, it is important to point out that such reasonable assessment of necessity by the victim State does not imply that it opens the door to abuses of the right of self-defence. In other words, the victim State must be cautious at the moment of assessing whether or not the necessity really exists.

In parallel to the necessity requirement, at the same time, International Law obliges any reaction in the right of self-defence to be proportionate with the cyber attack. In other words, it can neither be unreasonable nor excessive. In this regard, *Tallinn Manual 2.0* states that proportionality refers to how much cyber force is permitted when it is deemed necessary, affirming that

> "{this} criterion limits the scale, scope, duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defence. It does not restrict the amount of force used to that employed in the armed attack since the level of force needs to successfully amount a defence is context-dependent; more force may be

[1263] *Tallinn Manual 2.0, op. cit.,* rule 72, par. 4.

[1264] *Ibid.*

> necessary, or less force may be sufficient, to defeat the armed attack or repel one that is that is imminent"[1265].

Then, in this regard *Tallinn Manual 2.0* explicitly declares that necessity and proportionate requirements work together while any reaction in excessive force is not legitimate.

In fact, proportionality implies that the degree of cyber-force employed is limited in magnitude, intensity and duration to what is reasonably necessary to counter the attack. In this sense, proportionality

> "applies both to whether a given level of cyber-force is appropriate as response to a particular grievance (as a part of the law of the use of force, *jus ad bellum*) and whether a given cyber action as appropriate in light of its objective and the damage/casualties that will result"[1266].

In this context, legal experts believe that in the exercise of the right of self-defence, States must bear in mind both the necessity and proportionality requirements in order to use force properly. However, it does not mean that they shall use the same means and targets against the offender[1267]. Necessity and proportionality requirements in the right of self-defence are two sides of the same coin and are narrowly linked together[1268]. In this regard, views of most scholars are equivalent with the expression that "cyber attack can be responded with kinetic force, as much as kinetic force can be responded with a stronger act of kinetic force, as long as it is proportional to the effectiveness of the self-defence"[1269]; then, proportionality of the response is not purely limited to a cyber response[1270]. In this

---

[1265] *Tallinn Manual 2.0, op. cit.,* rule 72, par. 5.

[1266] JOYNER, C. C.; LOTRIONTE, C., "Information warfare…", *op. cit*., p. 858.

[1267] US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment ..., op. cit.,* May 1999, p. 16; ILA, *Draft Report on aggression and the use of force, op. cit*., 2016, p. 18.

[1268] RUYS, T., *'Armed Attack' ..., op. cit.,* p. 123.

[1269] DECOULARE-DELAFONTAINE, N., "Cyber attacks on nuclear...", *op. cit*., p. 24.

[1270] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense …", *op. cit*, p. 121; in this regard Roscini affirms that "Cyber operation does not mean in kind and allows both a kinetic and a cyber response to a cyber attack, as well as a cyber response to a kinetic attack", ROSCINI, M., *Cyber operation*…, *op. cit*., p. 90.

direction, *Tallinn Manual 2.0* explicitly illustrates that "there is no requirement that the defensive force be of the same nature as that constituting the armed attack. Therefore a cyber use of force may be resorted in response to a kinetic armed attack, and vice versa"[1271].

Also, the US *DoD Cyberspace Policy Report* proclaims that self-defence includes effective deterrence and response with all necessary means against any hostile acts on cyberspace; hostile acts include all significant cyber attacks against the US economy, government or military to which the US may respond with *cyber and/or kinetic capabilities*. In addition, it asserts that cyberspace operations have such a dynamic and sensitive nature that makes them difficult to choose specific capabilities[1272].

Thus, based on the inherent rights of self-defence, States have the right to use force by all necessary means, information, military or economic to defend their nation and interests. It is noticeable that if the originator of a cyber attack is invulnerable to a cyber operation response, then there is no reason to preclude kinetic operations as attempts to cease and deter the attacker[1273]. In this sense, Roscini, regarding the type of reaction against cyber operations, affirms that "a response in-kind against a cyber attack may not always be possible or effective, either because the victim State does not have the technology to hack back or because the aggressor is a low-technology State, or a non-State actor with no digital infrastructure to hit"[1274]. Therefore, in the right of self-defence, the State can react by all means necessary to protect its nation and interests.

In relation to what level of force is allowed to respond to a cyber attack, , on one side, it seems very difficult, if not impossible, to assess how much force in cyber terms it is necessary and proportionate to such attack since the modern security threats under

---

[1271] *Tallinn Manual 2.0*, *op. cit.*, rule 72, par. 5.

[1272] US, DoD CYBERSPACE POLICY REPORT, *A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, November 2011, p. 4, *op. cit.*

[1273] *Tallinn Manual 2.0, op. cit.,* rule 72, par. 6; and ROSCINI, M., *Cyber operation…*, *op. cit.*, p. 90.

[1274] ROSCINI, M., *Cyber operation…*, *op. cit.*, p. 90.

advanced technology, changed the nature of the conflict[1275]. On the other side, to limit cyber reaction to the intended target in self-defence by using a computer application is really hard when they are sending malware through cyberspace which "might spread uncontrollable"[1276]; for example, when Iran nuclear facilities were the target of *Stuxnet* virus, over 40 per cent of the computers affected by such virus, were outside Iran[1277]. Hence, following the proportionality requirement in cyber space is problematic because it is difficult to limit the effects of the response in self-defence only to the concerned State or to the non-State actor sanctuary[1278].

As a result, self-defence against cyber operations is highly dependent on the effects of the cyber attack. Therefore, we are facing challenges to assess proportionate force, especially when the effects of some cyber operations are not at the moment and it may take some time to its effects to appear, such as activities of the worm *Stuxnet*[1279]. In fact, both the speed and hidden nature of cyber attacks make it difficult to account magnitude and consequences of such attacks to react in the right of self-defence to meet the proportionality criteria[1280]. Although, the proportionality requirement is a factor to justify the legality of the use of force in the right of the self-defence, a disproportionate cyber reaction would not *per se* turn the reaction in self-defence into an unlawful reprisal, "only renders the State responsible of an act of excess (or abuse) of self-defence"[1281].

Moreover, applying the requirement of necessity and proportionality is especially difficult in the field of anticipatory self-defence[1282]. It seems that in some circumstances the right of

---

[1275] SAMPSON, E., "Necessity, proportionality and distinction in nontraditional conflicts" in FORD, C. A.; COHEN, A. (eds.), *Rethinking the law of armed conflict in an age of terrorism*, Lexington Books, 2012, p. 195-214, at p. 195.

[1276] ROSCINI, M., *Cyber operation*…, *op. cit*., p. 91.

[1277] O'CONNELL, M., E., *et al*., "Cyber security…", *op. cit*., p. 7.

[1278] GARDAM, J. G., "A role for proportionality in the war on terror", *NJIL,* 74, 2005, p. 17.

[1279] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit*, p. 121; and HOISINGTON, M., "Cyberwarfare…", *op. cit*., p. 452.

[1280] ROSCINI, M., *Cyber operation*…, *op. cit*., p. 90.

[1281] RONZITTI, N., "The expanding law of self-defence", *Journal of Conflict and Security Law*, 11(3), 2006, p. 343-359, at p. 355.

[1282] CHRISTODOULIDOU, T.; CHAINOGLOU, K., "The Principle of proportionality...", *op. cit*., p. 84-88.

self-defence can be applicable when a victim State suffers a severe cyber attack and there are no reasonable doubts that the aggressor is preparing an imminent cyber attack; in this situation, the imminent danger must be clear for the victim State provided that it is the last chance and it might be too late to react if the State hesitated to respond. At the same time, *proportional-limited* cyber or military force responds to the aggressor to disrupt or destroy their base or system that has caused or cause further cyber attack is acceptable under the recent *ius ad bellum* practice[1283].

In short, the right of self-defence is available to repel cyber attacks, but there are serious discussions about when (necessity) and how (proportionality) to exercise this right, because International Law does not dictate a particular criteria to perform such right of self-defence. Regarding the nature of cyber space, any cyber response in the right of self-defence is difficult following the proportionality requirement.

2. *Immediacy*

The requirement of immediacy intrinsically suggests that the activation of self-defence must not be too late[1284]. As mentioned *supra*, the criteria of immediacy distinguish the use of force under the right of self-defence from retaliation. In this sense, *Tallinn Manual* 2.0 asserts that "factors such as the temporal proximity between attack and response, the period necessary to identify the attacker, and the time required to prepare a response are relevant in this regard"[1285].

[1283] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit*, p. 121.

[1284] DINSTEIN, Y., "Computer network attacks…", *op. cit.*, p. 110; and SHARP, W, G*., Cyber space…, op. cit.,* p. 132.

[1285] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 12.

a) *The problem of quick identification of cyber attackers and a posteriori response*

International Law does not authorize to use force in the right of self-defence to cross international borders, unless a State is victim of an armed attack by another State or non-State actors placed in the territory of another State. As we have seen, on one side, to assess the necessity requirement, an attack must be attributed to a specific source and the hostile intention must be behind such attack to justify the right of self-defence[1286]. On the other side, in the context of cyber attacks, anonymity is one of the features of the perpetrators of such attacks because they will probably be unidentified[1287]. Anyone who studies cyber attacks, usually knows that the attacker goes to great lengths to hide its identity or use tricky ways to curve the origin of the attack. This makes it more difficult or almost impossible to discern the attribution of the attack quickly and accurately.

This difficulty is confirmed by the US *Deputy Secretary of Defence* Lynn who states that "it is difficult and time consuming to identify an attack perpetrator. Whereas a missile comes with return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all"[1288]. The nature of electronic informational infrastructure and limits of forensic capabilities make it technically impossible to attribute an attack to the ultimate part responsible[1289].

Likewise, the challenges to use the immediacy criteria in cyber operations have been confirmed by *Tallinn Manual 2.0* where it remarks that when a "cyber armed attack has occurred or is occurring may not be apparent for some time. This maybe so because the cause of the damage or injury has not been identified", or may be, "the initiator of the attack

[1286] HOISINGTON, M., "Cyberwarfare…", *op .cit.*, p. 450.

[1287] BRENNER, S. W., "'At light speed'…", *op. cit.*, p. 379.

[1288] LYNN, W. J., "Defending a new domain: the Pentagon's cyber strategy", *Foreign Affairs*, 89(5), 2010, p. 97-108, at p. 99.

[1289] GOLDSMITH, J., "The new vulnerability", *The New Republic,* 7 June 2010, p. 21-23, available at https://newrepublic.com/article/75262/the-new-vulnerability, {visited on 22 June 2018}.

is not identified until well after the attack"[1290]. This situation is obvious in operations of a worm, such as *Stuxnet*. Therefore, in this view, the criteria of immediacy to exercise the right of self-defence against *some* cyber operations cannot meet.

According to some scholars, there is "broadly view" on the immediacy criteria in the context of cyber attacks, especially when "there may be a time-lag of day, weeks, and even months between the original armed attack and the sequel of self-defence"[1291]. In this regard, "immediacy does not mean 'instantaneous' and must be applied *flexibly*"[1292], but "there must not be an undue time-lag between the armed attack and the exercise of self-defence in response"[1293]. In this direction, it is emphasized that "difficulties in quickly identify in attackers must not prevent a nation from being able to respond in self-defence. Rather, the law should permit an active response based on the target of the attack regardless of the attacker's identity"[1294]. Thus, in some cases, the lack of quick identification of the attacker, cannot prevent the victim State from exercising the right of self-defence.

Consequently, it seems reasonable that "State does not {…} forfeit its right of self-defence because it is incapable of instantly responding or is uncertain of who is responsible for the attack or from where the attack originated"[1295]. In this sense, some *flexibility* in assessing the immediacy to react against cyber attacks is required. It seems logical that, in some circumstances, the victim State requires time to gather sufficient evidence to accuse a specific State or non-State actor of conducting the cyber attack[1296]. Furthermore, in light of the nature of the cyber space, there is a time-consuming process regarding the effects of the cyber operation (effect-based approach) to qualify the cyber attack as armed attack, before

---

[1290] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 14.

[1291] DINSTEIN, Y., "Computer network attacks…", *op. cit.*, p. 110.

[1292] ROSCINI, M., *Cyber operation…, op. cit.*, p. 91 (italic is ours).

[1293] DINSTEIN, Y., *War, aggression…, op. cit.*, p. 252.

[1294] JENSEN, E.T., "Computer attacks…", *op. cit.*, p. 234; and SHULMAN, M. R., "Discrimination in the laws of information warfare", *Columbia Journal of Transnational Law*, 37, 1999, p. 939- 968, at p. 955-956.

[1295] GILL, T. D.; DUCHEINE, P. A., "Anticipatory self-defense…", *op. cit.*, p. 451.

[1296] ROSCINI, M., *Cyber operation…, op. cit.*, p. 91; and JENSEN, E.T., "Computer attacks…", *op. cit.*, p. 232-233.

conducting any reaction in the right of self-defence[1297]. In fact, due to the nature of cyber attacks, in most of the cases, the use of force in the right of self-defence would be exercised *posteriori*[1298].

b) *Anticipatory right of self-defence and cyber operations*

The ultimate purpose of the right of self-defence is to repel a cyber attack. In this sense, we must point out that the requirement of immediacy should not be confused with the *imminence* of cyber attack in the context of the anticipatory self-defence[1299].

As mentioned *supra*, there is a substantial legal support of anticipatory right of self-defence when there exists a persuasive evidence that an armed attack is *imminent*. In anticipatory self-defence "the key to the determination of a necessity is imminence"[1300]. In this regard, the US *Standing Rules for the Use of Force* provides that "the determination of whether the use of force against US forces is imminent will be based on an assessment of all facts and circumstances known to US forces at the time and may be made at any level. Imminent does not necessarily mean immediate or instantaneous"[1301].

In the context of cyber attacks, the State is not required to wait inactively until the actual armed attack occurs, and therefore it can use proportional forces to repel the imminent attack[1302]. Nowadays, it does not seem legitimate to resort to the right of self-defence is only against consummated attacks, especially in a world with an increasingly number of cyber attacks and the development of a more complex technology[1303].

[1297] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit*, p. 121.

[1298] See ROSCINI, M., *Cyber operations…, op. cit*., p. 91; and CERVELL, M. J., *La legítima defensa…, op. cit*., p. 305.

[1299] ROSCINI, M., *ibid,* p. 91.

[1300]DEWEESE, G. S., "Anticipatory and preemptive self-defense…", *op. cit*., p. 87.

[1301] US CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 3121.01B, *Standing Rules of Engagement (SROE)/Standing Rules for the Use of Force (SRUF) for U. S. Forces*, 13 June 2005, p. 84, available at http://www.loc.gov/rr/frd/Military_Law/pdf/OLH_2015_Ch5.pdf, [visited on 22 May 2018].

[1302] *Tallinn Manual 2.0…, op. cit.,* rule 73, par. 2.

[1303] CERVELL, M. J., *La l legítima defensa…, op. cit.,* p. 169.

In this respect, primarily, if a State becomes aware that its systems will be under the effects of a cyber attack, it can take passive cyber defence measures to neutralize the threat. Then, if all means of neutralizing the cyber attack fails, or the State has reasonable evidence that the incursion in the system is part of an overall attack, it can resort to the anticipatory self-defence[1304]. In fact, the speed of data transmission in cyber space is adapted *instantly* and no *moment for deliberation* of elements of *Caroline doctrine* are part of the prerequisites to justify the anticipatory self-defence[1305].

The use of the anticipatory self-defence in the case of cyber operation is more difficult than in the case of an attack by kinetic means where there normally are intimations of an impending attack, such as propaganda, bellicose statements or clear threats as movement of forces in the border[1306]. Thus, there are some challenges to the application of the traditional temporal criterion in the field of cyber operations because it is launched without any warning of the imminent attack; the time between the launching of the cyber attack and the occurrence effect are almost a matter of seconds, provided that the mere clicking of a button or the moving of a mouse through the screen can constitute instant damage[1307]. In this sense, the requirement of imminence in anticipatory self-defence in cyber operations "would invariably be difficult to meet, if not impossible"[1308], depriving State to thwart the *initial attack*, and then workable defences can be limited to passive defence measures, such as firewall and antivirus software[1309]. Also, when a cyber attack is imminent, it is very complex to notice if it has sufficient gravity to identify it as an *armed attack* and therefore authorize the anticipatory self-defence[1310].

[1304] TSAGOURIAS, N., "Cyber attacks…", *op. cit.*, p. 232.

[1305] TODD, G, H., "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition", Air Force Law Review, 64, 2009, p. 65-107, p. 99.

[1306] ROBERTSON, H. B., "Self-defense against…", *op. cit.*, p. 138.

[1307] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 167; and ROBERTSON, H. B. "Self-defense against…", *op. cit.,* p. 139.

[1308] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit*, p. 121.

[1309] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 167.

[1310] ROBERTSON, H. B., "Self-defense against…", *op. cit.,* p. 139.

Therefore, the most critical challenge to analyse in the anticipatory self-defence is the determination of the imminent threat[1311]. To find out whether a cyber attack is imminent, would be based on the assessment of all circumstances in time. If the target State has evidence that the cyber attack is imminent, and there is reasonable evidence of harm to its critical infrastructures or loss of human life, the exercise of proportional response in the frame of anticipatory self-defence is lawful[1312].

Likewise, the US DoD in the *Cyber Strategy* argues that "the US military may conduct cyber operations to counter an imminent or on-going attack against the US homeland or US interests in cyberspace. The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life"[1313]. Then, the US explicitly accepts the anticipatory right of self-defence against imminent cyber attacks and the international community recognizes that "the traditional conception of what constitutes an 'imminent' attack must be understood in light of modern-day capabilities, techniques, and technological innovations of terrorist organizations"[1314].

Also, the majority of scholars assert that "anticipatory self–defence is a lawful exercise of right of self-defence when exercised in response to a manifest and unequivocal imminent threat of attack in proximate future against a designated target State or States, as these criteria are laid down in the Charter and are contained in customary International Law"[1315].

[1311] DEWEESE, G. S., "Anticipatory and preemptive self-defense...", *op. cit*., p. 81.

[1312] ROBERTSON, H. B., "Self-defense against …", *op. cit*., p. 138; and HOISINGTON, M., "Cyberwarfare…", *op. cit*., p. 453.

[1313] US, DoD, *Cyber Strategy*, 17 April 2015, p. 5*, op. cit*.; this view is also repeated by the US Department of State, legal advisor Koh, who asserts that inherent right of self-defence is applicable against cyber attack "that amount to an armed attack or imminent threat thereof", KOH, H. H., "International Law…", *op. cit*., p. 4.

[1314] US, *Report on the legal and policy frameworks guiding the United States' use of military force and related national security operations*, The White House, December 2016, p. 9; available at https://www.justsecurity.org/wp-content/uploads/2016/12/framework.Report_Final.pdf, [visited on 2 January 2018].

[1315] Among others see GILL, T. D.; DUCHEINE, P. A. L., "Anticipatory self-defense…" *op. cit.,* p. 464-465.

In particular, *Tallinn Manual 2.0* affirms that "the right of use of force in self-defence arises if a cyber armed attack occurs or is imminent"[1316], and accepts that all *reasonably foreseeable consequences* of a cyber operation must be taken into account to qualify such operation as an armed attack; for instance, those cyber operations that targeted the water purification plant and gave rise to sickness and death by contaminated water are foreseeable and therefore can reach the level of armed attack[1317]. Thus, the State has the right to resort to the right of self-defence if there is a reasonable assessment that an armed attack is imminent.

As has been observed, in order to justify the anticipatory self-defence, States must provide at least minimum "clear and convincing" evidence of imminent attack to justify the right of self-defence. In this regard, some powerful States probably pursue a more *flexible approach* of imminence while, on the contrary, other States that fear possible abuses support a stricter temporal notion of imminence[1318]. For instance, the UK accepts that *imminence* in the International Law of self-defence "must be interpreted with a degree of *flexibility*, in light of modern conditions and in particular the fact that we live in an era of instantaneous communication"[1319].

Another challenge in the application of anticipatory self-defence against the cyber attack concerns the capacity of the target State to identify the prospective capability of the attacker and ascertain its intentions. As mentioned, without physical indicators, it is certainly difficult to identify the attacker, intent, and nature of the threat to choose the type of reaction in accordance with the necessity and proportionality criteria, along with the reasonable degree of certainty[1320]. In this regard, in the absence of an associated kinetic

---

[1316] *Tallinn Manual 2.0, op. cit.,* rule 73.

[1317] *Ibid,* rule 71, par. 13; ILA, *Draft Report on aggression and the use of force, op. cit.,* 2016, p. 18.

[1318] See ROSCINI, M., *Cyber operations*…, *op. cit*, p. 80.

[1319] UK, The Government's policy on the use of drons for targeted killing, Second Report of Session 2015–16, HC 574, HL Paper, 10 May 2016, p. 46 (italic is ours), available at https://publications.parliament.uk/pa/jt201516/jtselect/jtrights/574/574.pdf, [visited on 2 April 2018].

[1320] GILL, T. D.; DUCHEINE, P. A. L., "Anticipatory self-defense…", *op. cit*., p. 466; and O'CONNELL, M., E., *et al*., "Cyber security…, *op. cit*., p. 6; see also HOISINGTON, M., "Cyberwarfare…", *op. cit*., p. 450-453.

attack, "anticipatory self-defence by cyber or kinetic means against an imminent standalone *cyber* armed attack will be extremely difficult to invoke in practice"[1321].

The most likely use of anticipatory self-defence against cyber operations would be when cyber operations do not amount to an armed attack, but they are precursors of an armed attack by kinetic means and/or more severe cyber attacks. In fact, the electronic battlefield has the leading role in modern conflicts, where States attempt by means of cyber attacks to destroy the enemy's electronic command and control, intelligence, communication and weapon control network, prior to resorting to the kinetic attack. In this sense, even if the use of cyber operations does not reach the level of an armed attack, the victim State can resort to the anticipatory self-defence against an imminent attack through conventional means; for instance the Russian cyber attack to Georgian Government websites in 2008 before the beginning of the conflict, or cyber operations by Israel to disable Syrian air defence systems prior to the 2007 air attack to nuclear power plant. Therefore, if cyber attacks are a prelude (*positional manoeuvre*) to a kinetic attack, the use of anticipatory self-defence is lawful[1322].

It seems that the imminence of the attack is not only based on the time factor, but also on other circumstances that must all be evaluated in every particular case[1323]. In fact, the imminence character in a cyber attack "depends on the intensity of the attack, the target of the attack, the reaction time required in order to successfully pre-empt the attack, and the speed with which the damage may move throughout the computer networks"[1324].

The majority of scholars in *Tallinn Manual* reject the strict temporal analysis and refer to the "last feasible window of opportunity" standard; according to this standard, States have

---

[1321] ROSCINI, M., *Cyber operations…*, *op. cit*, p. 79.

[1322] TSAGOURIAS, N., "Cyber attacks…", *op. cit*., p. 232; ROBERTSON, H. B., "Self-defense against ….", *op. cit*., p. 139; DEWEESE, G. S., "Anticipatory and preemptive self-defense…", *op. cit*, p. 89; and APPLEGATE S. D., "The principle of maneuver in cyber operations", in CZOSSECK C., *et al.* (eds.), *2012 4th International Conference on Cyber Conflict* (CYCON 2012), NATO CCD COE, 2012, p. 183-195, at p. 189, where point out that positional manoeuvre as "the process of capturing or compromising key physical or logical nodes in the information environment which can then be leveraged during follow-on operations".

[1323] ROSCINI, M., "World wide warfare…", *op. cit*., p. 122.

[1324] JOYNER, C. C.; LOTRIONTE, C., "Information warfare…", *op. cit*., p. 860.

the right to use anticipatory self-defence against cyber or kinetic armed attack "when attacker clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts" [1325]. The realization of the *last opportunity* to use effective defence in the anticipatory self-defence depends on the evaluation of information available at that time based on good faith[1326].

Moreover, in this context, Deweese points out that "imminent in the cyber domain must not be tied to a strict temporal analysis but should accommodate a broad window of opportunity approach {…} victim State may not always know the intent of an adversary who implants malicious malware on the victim State critical infrastructure"[1327]. In the same direction, the majority of experts in *Tallinn Manual 2.0* assert that the anticipatory self-defence may act

> "only during the last window of opportunity to defend itself against an armed attack that is forthcoming. This window may present immediately before the attack in question, or, in the same cases, long before it occurs.{...} The critical question is not the temporal proximity of the anticipatory defensive action to the prospective armed attack, but whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts"[1328].

In contrast to the narrow Webster's view "while a restrictive construction {of imminence} may have made sense in the nineteenth century, the nature of warfare has evolved dramatically since then". In this sense, "in the twenty–first century, the means of warfare are such that defeat, or at least a devastating blow, can occur almost instantaneously"[1329]. Thus, the "restrictive approach to immanency run counters to the purposes animating the

---

[1325] SCHMITT, M. N., (ed.), *Tallinn manual, op. cit.,* rule 15, par. 4; see also DEEKS, A. S., "Taming the doctrine of pre-emption" in WELLER, M., *The Oxford Handbook of the use of force in International Law*, OUP, 2015, p. 661-678, at p 678.

[1326] ROSCINI, *Cyber operations…, op. cit*., p. 79.

[1327] DEWEESE, G. S., "Anticipatory…", *op. cit*., p. 81.

[1328] *Tallinn manual 2.0…, op. cit.,* rule 73, par. 4.

[1329] SCHMITT, M. N., "Preemptive strategies in International Law", *MJIL*, 24(2), 2003, p. 513-548, at p. 534.

right of self-defense"[1330]. Then, if intelligence service of one State receives undeniable information that another State is preparing to launch a cyber operation against a critical infrastructure in the next two weeks with serious destruction effects, but intelligence services do not have specific information about a particular place or time, as a result of the imminent attack, the anticipatory self-defence would be lawful[1331].

There is a distinction between preparatory actions and conducting the initial phase of an attack; for instance, merely obtaining capabilities for a future armed attack cannot meet the requirement of imminence[1332], but if this preparation is followed by an initial phase, such as the laying of naval mines in the shipping routes of the target State, it can clearly constitute an armed attack; also, the insertion of a logic bomb will be qualified as an imminent armed attack if the specific conditions for its activation are likely to occur[1333]. Anyway, the lawfulness of the anticipatory self-defence can be determined by the reasonableness of the victim State when assessing the situation[1334]. It means that the victim State has the right to react in the right of self-defence against an armed attack whenever a cyber attack is qualified as an armed attack, albeit the "response are assessed as of the time to took action, not *ex post facto"*[1335].

Nevertheless, we must point out that these broad rules on anticipatory self-defence could open the door to abuses by potential victim States. In this sense, according to the more restrictive view, the mere installation of vulnerabilities in computer systems of another State that might be used later as a cyber attack, *per se* cannot justify the right of the anticipatory self-defence[1336]. Also, it seems that the exercise of the anticipatory self-defence cannot be necessary if such vulnerabilities are discovered and neutralized by passive

---

[1330] *Ibid*.

[1331] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 6.

[1332] In this regard, "raining, wargaming and advance preparations do not cross the red line of an armed attack" to resort of the right of self-defence, DINSTEIN, Y., *War, aggression…, op. cit*., p. 232.

[1333] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 7.

[1334] *Ibid,* par. 8.

[1335] SCHMITT, M. N., "Cyber operations…", *op. cit*., p. 168.

[1336] ROSCINI, *Cyber operations…, op. cit,* p. 79.

cyber-defence[1337]. In this sense, States can resort to the anticipatory self-defence "if all other means of neutralizing the cyber threat fail"[1338].

A critical issue to be addressed is how to assess the length of time that the right of self-defence can continue following the completion of a particular armed attack. In this sense, if an armed attack starts with a wave of cyber operations against a victim State, resorting to the right of self-defence by this State does not necessarily have to finish with the termination of those cyber operations. If it is reasonable that further cyber operations are likely to follow, the victim State can continue acting in self-defence[1339]. However, if the continuation of such cyber operations is not reasonable, "any further use of force, whether kinetic or cyber, is liable to be characterized as mere retaliation"[1340].

As mentioned earlier, the *reasonableness* standard would apply in the anticipatory self-defence against imminent cyber attacks. In this sense, Schmitt believes that there is not any necessity to ascertain *clearly* future actions of States or non-State actors[1341]. In this direction, some scholars believe that, regarding the unique nature of cyber attacks, International Law should afford protecting States who initiate a good-faith response to an armed attack when

> "State survival may depend on an immediate, robust, and aggressive response; therefore International Law should not impose an inflexible requirement on State to fully satisfy the traditional necessity requirements when acting in self-defence of vital State interests. The law should evolve to recognize a State's inherent right to self-defence, including anticipatory self-

[1337] *Ibid*, p. 79.

[1338] TSAGOURIAS, N., "Cyber attacks…", *op. cit.*, p. 232.

[1339] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 13.

[1340] *Ibid.;* see also SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 116.

[1341] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 168.

> defence, in response to cyber attack, especially when the attack targets critical national infrastructure"[1342].

Then, regarding the nature of the cyber attack, an inflexible requirement to exercise the anticipatory self-defence could endanger the survival of the State when the attacker targets are the critical infrastructures of such State.

Moreover, Jensen affirms that "in this technologically advanced era in which a simple keystrock can have an immediate lethal impact, leave no time for other currently acceptable defensive measures, the law must evolve to allow a nation to defend itself effectively"[1343]. Hence, it seems that to cope with cyber attacks with immediate lethal effects, the authorization of the victim State to resort in anticipatory self-defence is necessary.

To assess whether a potential State or non-State actor has the intention to attack and has the capability to conduct such attack, it requires *reasonableness*. In this regard, the use of anticipatory self-defence by a victim State is inevitable before it loses the opportunity to guarantee its survival. Hence, any conception with higher threshold to justify the use of anticipatory self-defence against a cyber attack, would deprive States from the right of self-defence[1344]. In this direction, to reach the conclusion that a cyber operation constitutes an armed attack, it has to be evidenced by demonstration of its *hostile intention.* In this situation,

> "if the victim State is to have any reasonable hope of fending it off. Consider a State's introduction of cyber vulnerabilities into another State's critical infrastructure. Such an action might amount to a use of force, but the victim-State may not react forcefully until it reasonably concluded that (1) its opponent has decided to actually exploit those vulnerabilities; (2) the strike is likely to generate consequences at the armed attack level; and (3) it must

[1342] HOISINGTON, M., "Cyberwarfare…, *op. cit.*, p. 453.

[1343] JENSEN, E.T., "Computer attacks…", *op. cit.*, p. 231.

[1344] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 168.

act immediately to defend itself. Until arriving at these conclusions, the victim State's response would be limited to non-forceful measures, including countermeasures and referral of the matter to the Security Council"[1345].

In fact, the requirement of immediacy is based on a test of reasonableness in respect of the circumstances prevailing at any situation[1346].

In this context, it is important to remember that any preventive action against an armed attack is unlawful. This rule is also applicable in the context of cyber attacks. Thus, the *last feasible window of opportunity* to use force in anticipatory self-defence must not be interpreted as the use of preventive strike against another State or non-State actors. Also, if the hostile State merely has capability to launch a cyber attack, even with a possible devastating result, the potential victim State does not have the right to recourse to the use of force and cannot be justified under the anticipatory self-defence since it falls under the unlawful preventive self-defence[1347].

Even if another State has shown the intent and opportunity to carry out an armed attack, until it reaches the *last opportunity* resort to exercise the right of self-defence effectively, the recourse to self-defence by the potential victim State will be unlawful[1348]. However, after the past experience of some cyber operations that have occurred or are secretly occurring for a long time now without identifying its damages or injuries, States and scholars realized that the last opportunity resort to use of force is almost impossible; for instance, the employment of worm *Stuxnet*[1349].

Therefore, meeting all the requirements to justify the right of self-defence in the context of cyber attacks is very difficult if not impossible; this challenge derives from the complexity

---

[1345] *Ibid*, p. 166.

[1346] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 13.

[1347] SCHMITT, M. N., "Cyber operations…", *op. cit.*, p. 166.

[1348] *Tallinn Manual…, op. cit.,* rule 15, par. 7; and *Tallinn Manual 2.0…, op. cit.,* rule 73, par. 11.

[1349] *Tallinn Manual 2.0, op. cit.,* rule 73, par. 14.

of cyber operations in relation to the amount of time needed to attribute the attack[1350], the difficulty to notice their effects and the obstacles to identify the attacker and its intentions on time before conducting a cyber attack that authorizes the victim State to resort to the anticipatory self-defence[1351]. Then, for the moment, although International Law has attempted to confront cyber threats with the traditional principle of the use of force, in light of special characteristics of cyber threats, it is necessary to reinforce bilateral, regional and international cooperation, promote the important role of the UN and introduce new rules that have been suggested by some countries like Russia, China, Tajikistan and Uzbekistan[1352]. However, in this field, some States may prefer to use existing rules. Anyhow, over time, we will see in which way the international community develops the principle of the use of force, may be with a treaty or with new interpretations[1353]. Regarding the interpretation, it appears that the most feasible solution would be the ICJ interpretation of the international rules according to the new reality of the XXI century or to wait for new international customary law to admit the right of self-defence against imminent and non-State actors[1354].

[1350] HADJI-JANEV, M.; ALEKSOSKI, S., "Use of force in self-defense…", *op. cit*, p. 121.

[1351] HOISINGTON, M., "Cyberwarfare…, *op. cit.*, p. 451.

[1352] UNGA, Doc. A/66/359 "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", 14 September 2011, (j); see also CERVELL, M. J., *La legítima defensa…, op. cit.,* p. 311.

[1353] CERVELL, M. J., *La legítima defensa…, ibid.,* p. 320.

[1354] *Ibid*, p, 320-322.

CONCLUSIONS

FIRST. The technological development in the field of cyber activities has introduced new threats to the national security of States. International Law in general and the UN Charter in particular have always been mainly engendered to cover kinetic activities. The UN Charter was written before the internet and, as a result, cyber operations present a unique and real challenge to the traditional definition of what constitutes a use of force. Historically, technology has preceded the law; hence, nowadays International Law is behind internet and technology age. As technology keep becoming more sophisticated, the problems in the laws governing cyber attacks and cyber security grow correspondingly. Therefore, cyber attacks and its specific characteristics present essential challenges. To cope with them, new translations on fundamental rules of International Law regarding the cyber domain are required. Indeed, applying pre-existing legal principles to modern technology may raise the question of whether such rules are sufficiently clear in light of the technology's specific characteristics.

Despite this difficulty, the serious and pervasiveness of the threat of new technology demands that the international community reaches a consensus on both the meaning of cyber attack as an armed attack within the *jus ad bellum* paradigm, and the options, such as the right of self-defence, which are available to victim States to counter such attacks. However, International Law has serious flaws in its application against cyber operations, uncertainty of not knowing when a cyber attack constitutes an *armed attack* and difficulties when attributing such attacks to States or non-State actors. Therefore, these continuous flaws create a loophole from where hackers can strike. Moreover, while a cyber operation that unequivocally breaches International Law may yet have to occur, the current absence of a legal framework enables actors deserving punitive action to operate without accountability. It also leaves the door open for future potential abuses.

In this situation, the cyber age will expose State's sovereignty to new challenges since cyber attacks represent new ways of intruding on the sovereign prerogatives of States. Thus, international peace and security will face serious threats unless States have the ability to respond in self-defence to cyber attacks without being restrained by outdated

interpretations of International Law governing the principle of the prohibition of the use of force. It seems that only a broader standard will deter substantial intrusions on sovereignty through the use of cyber operations.

Despite the complex problems cyber technology raises to the International Law, after the research, our task in the next conclusions is to offer solutions to cope with the new threats caused by the digital age which International Law does not give explicit solutions to. It seems that universal treaties would be the most suitable instrument to regulate the upcoming issues, provided that in the field of modern technology it is very difficult to establish clear rules through customary International Law. However, it is important to keep in mind that among the international community, States, specially from developed countries, are hesitating to set new universal rules to regulate cyber space activities. This is because, in chaos arena, on one side, they have more freedom to conduct cyber operations to pursue their interests and, on the other side, it opens the door to abuses of the right of self-defence against cyber attacks.

SECOND. One of the most important achievements of international community during the XX Century has been the prohibition of the threat or use of force in article 2(4) of the UN Charter. This principle of the prohibition of the use of force is a fundamental rule of International Law admitted in the context of *international relations,* but it is only actionable in cases where there is no *armed conflict.* Therefore, in the context of cyber operations, those cross-border cyber attacks that are carried out directly or indirectly by States against other States can violate the principle of the prohibition of the use of force.

Thus, the principle of the prohibition of the use of force is applicable in *inter-State* relations and is not usable in the framework of internal affairs of States, except for situations where the *intra-State* conflicts become internationalized. Such conflicts particularly refer to direct and indirect use of force by State in internal conflict of another State through assistance or logistical support of rebel groups. However, the presence of foreign troops in an internal conflict of another State by consent of the host State cannot breach such principle. Also, some police measures of States to exercise its competence against individuals, inside or outside its territory, who break the law, cannot violate this principle.

THIRD. In the scope of the principle of the prohibition of the use of force there is *no restrictive* view. Therefore, the principle includes any kinds of force regardless of whether forces are against *territorial integrity* or *political independence* of other States. In this sense, even minor violations of State boundaries can breach this principle. In fact, all use of force that is inconsistent with the maintenance of international peace and security can violate such principle. After the adoption of the UN Charter, the prevailing view on the meaning of force over the years was limited to an *armed force*, but whereas International Law is *dynamic* rather than static, in conformity with the deleterious effect-based approach, the prohibition of the use of force can comprise non-military force when its level of harmful effects reaches the amount of an armed force. In this regard, biological and chemical weapons or intense cyber operations with capacity to destroy life and properties can violate the principle of the prohibition of the use of force.

According to modalities of the use of force upon graveness or scale and effects of the use of force, it is necessary to distinguish between *the most grave forms* and *other less grave forms* of the use of force. In this context, aggression and particularly the armed attack are the most grave forms of use of force, while other actions below the thresholds of aggression are less grave. Thus, all cyber operations with the analogous *scale* and *effects* to other kinetic or non-kinetic actions are accepted as use of force. In relation to the prevailing view, those cyber operations that cause or are likely to cause physical damage to property, loss of life or injury to persons, can violate the principle of the prohibition of the use of force. In contrast, other cyber activities, such as computer–based espionage and intelligence collection, cannot violate such principle because they are not able to cause direct or indirect destructive consequence equal to a military attack or armed force.

FOURTH. According to the prevailing view, political, diplomatic or economic coercions, cannot transgress the principle of the prohibition of the use of force. This approach was evident by the UN drafters and the international community in the last decades. However, recently, with the appearance of new non-armed force threats (chemical, biological, nuclear weapons, drones or cyber technology), new debates have arisen among the doctrine based on the effective approach (scale and effect criteria). In this sense, scholars have accepted that the meaning of force in the principle of the prohibition of the use of force includes

armed force as well as non-armed force. Then, nowadays, to maintain that the economic coercions, with destructive effects, cannot violate the principle of the prohibition of the use of force, would be incompatible with the scale and effect criteria, which is accepted by most of the doctrine.

In this regard, it seems that the most powerful States, based on their national interests, have a contradictory approach on non-armed force. On one hand, they are interested in maintaining a narrower interpretation view on the concept of force under the prohibition of the use of force, not including economic coercions. On the other hand, due to their vulnerability from modern technologies, particularly cyber attacks, in the last decades they have accepted a wide view on the notion of armed attack under article 51 of the UN Charter. Thus, when a non-armed force has high graveness effects, it can constitute an armed attack under article 51 of the UN Charter and grant the right of self-defence against such attacks.

To our understanding, cyber operations that are analogous to political, diplomatic and economic coercions, cannot violate the principle of the prohibition of the threat or use of force. However, in situations where the economic coercion, particularly through cyber attacks, constitutes such a serious pressure to a State that make impossible its normal life (for instance, some massive cyber operations that cripple the State's economy), this kind of coercions would violate such principle. Furthermore, such economic coercions with as disruptive and destructive effects as an armed force, can constitute an armed attack to justify the right of self-defence under article 51 of the UN Charter,

FIFTH. Article 2(4) of the UN Charter does not only explicitly prohibit the use of force, but also forbids the threat of force in international relations. Nevertheless, contrary to the use of force, there is a *restrictive view* on the prohibition of *threat of force* in article 2(4) rather than in the *threat of peace* under article 39. Then, in contrast to the meaning of *threat of peace* that has broad significance, the *threat of force* in article 2(4) has a restrictive signification. Hence, to prohibit the threat of force under article 2(4), the threat must be known and clearly directed to a target State; the mere supply of arms may well threat

international peace and security, but it would not necessarily violate the principle of the prohibition of the threat of force under article 2(4). Additionally, a mere verbal threat is not enough to breach such principle. Therefore, it explicitly or implicitly needs to intimidate another State by specific activities, such as concentration troops or removing and displaying forces, along with specific demands or hostile intentions.

It is noticeable that the prohibition of the threat of force in article 2(4) does not mean that the threat in each situation is prohibited. According to the presumptive legality, defensive threat of force is lawful if the use of force is legal. In this sense, defensive threat of force is legal if there exists the right of anticipatory self-defence. In the context of cyber operations, the mere acquisition of capabilities to conduct massive malicious cyber attacks without any direct threat to the target State or hostile intention of the threatener, cannot violate the principle of the threat of force in International Law. However, in practice, due to the nature of cyber space, the recognition of the threat of force in the context of cyber attacks is a tricky issue provided that, in cyber operations, the preparation to conduct a cyber attack cannot be visible, the threat through cyber operations are more independent from the cyber capabilities of the States and to find out the hostile intention prior to conducting the cyber attack is very difficult.

SIXTH. The right of self-defence is one of the exceptions to the principle of the prohibition of the threat or use of force that authorizes any State to resort to the use of armed force against another State. Contrary to the principle of the prohibition of the use of force, the prevailing view on the right of self-defence is a restrictive approach to prevent States to abuse this right since it constitutes an exception to the principle of the prohibition of the use of force in International Law.

According to the restrictive approach, on one side, to justify the right of self-defence, the security or existence of a State must be threatened; hence, attacks to nationals abroad, foreign diplomatic facilities or any similar attacks, are not serious threats to the existence of the State. In fact, attacks to nationals abroad or diplomatic facilities without the element of territory or the necessity criteria, cannot meet Main requirements (armed attack and necessity) to justify the right of self-defence. Since 1960, some interferer States in few cases

resorted to the right of self-defence to rescue nationals abroad (when the lives or health of its nationals are endangered in a foreign State and the host State is unable or unwilling to carry out rescue acts), but it is not possible to envisage such rescue operations in generalized practice.

Although, these limited military interventions to rescue nationals abroad have been totally tolerated by the international community, to our understanding, such interventions are opposite to the restrictive view on the exception of the use of force in self-defence which may authorize to maliciously take advantage of such right to carry out military interferences in the territory of another State.

However, the right of self-defence is allowed against an armed attack *as the most grave forms of use of force;* thus, the mere violation of the principle of the prohibition of the threat or use of force cannot justify the exercise of the right of self-defence. In this sense, in conformity with the modalities of armed force, only the aggression with high gravity can constitute an armed attack.

Nowadays, these grave modalities of force can also be carried out through cyber operations. In this regard, the development of technology has changed the scope of the battles in the international domain, provided that cyber operations high graveness against another State can constitute an armed attack. Despite the lack of a clear definition of gravity, under the effect-based approach, scale and effects of attacks are criteria to identify cyber operations as an armed attack. In this sense, those cyber operations that injure or kill people, destroy properties or severely disrupt the functioning of critical infrastructures of States with effects and consequences of high scale, can constitute an armed attack. Although espionage is not prohibited in International Law *per se*, it does not mean that cyber espionage cannot be qualified as use of force in some circumstances, particularly when it causes damage to cyber infrastructures that leads to technical malfunctions.

However, there is no general agreement on the definition of critical infrastructures. In this context, the majority of States have accepted that critical infrastructures refer to security, food, water, transportation, governmental and public services, health, banking and finance. In this era, it is important to point out that critical infrastructures are governed by governmental agencies as well as private companies; therefore, it makes no difference

whether these critical infrastructures are being managed by the government or private companies. Any cyber attack directly against critical infrastructures to cripple the State's and undermine its political and economic affairs for a long time can constitute an armed attack.

SEVENTH. To use force in the right of self-defence against another State, the armed attack must be attributed to such State. In this sense, an armed attack can be attributed directly to *de jure organ* of a State or indirectly to its *de facto organs. De jure organ* of a State includes all activities of the individual or collective entities which make up the organization of the State and act on its behalf. Cyber attacks by *de jure organ* of State often occur with cyber units against another State. To attribute an armed attack directly to the State organ, at first, the victim State must prepare appropriate evidence to substantiate such attack to that State. In the field of attribution, International Law does not determine specific evidentiary standards to clarify wrongful acts as originators of an armed attack, but *clear* and *convincing evidence* would be necessary to substantiate an armed attack to a specific State in order to prevent abuses of the right of self-defence. In the context of cyber attacks, the attribution is a very critical and complicated issue because of the technical nature of the cyber domain, where *anonymity*, *multi stage cyber attacks* and *speed* of cyber operations make it difficult to attribute a cyber attack to a State. These features indicate that most of cyber attacks are not clear and accessible as to provide conclusive evidence on who conducted the cyber attack. In this regard, whereas the clear and convincing evidence obliges a State to act advisedly, according to the reasonable standard, if the victim State has a rational evidence to attribute a cyber attack to an identified attacker, it has the right to resort to the self-defence or anticipatory self-defence. From this point of view, some casual factors, such as motivation, may be helpful. Even so, that alone is not sufficient to impute an armed attack.

In indirect armed attack by a State, *de facto organs* of State include, on one hand, entities that are empowered by the authorities of the State that are absorbed in the State apparatus. In the field of cyber attack, hackers can be members of parastatal entities or pubic, semi-public or privatized corporations that are empowered by domestic law to exercise some degree of governmental authority. Moreover, a cyber attack carried out by hackers hired by

State A to conduct attacks against State B, can be attributed to State A. According to the nature of the cyber space, States are more willing to use cyber operations by its State agents to conduct cyber attacks in order to camouflage its hostile acts.

On the other hand, entities may act on the instructions or under direction or control of a State; for instance, when the conduct of a person or group of persons under such control can be considered an act of that State. However, mere encouragement or support to non-State actors cannot attribute an armed attack to a State to justify the right of self-defence. The prevailing view in this context is the *effective control test,* which emphasizes on control over the act rather than control over the actors. The *effective control* approach represents a restrictive view to attribute an armed attack to another State to justify the exercise of the right of self-defence. In this sense, due to the nature of cyber space, the *effective control test,* on one side, prevents States from abusing the right of self-defence and, on the other side, it is more practical to cover individuals who are engaged in a State to conduct a cyber attack. According to the complexity of cyber operations, application of this general principle in each case, must be assessed on its own merits.

Also, there is another potential attribution to the State and that is when individuals conduct armed attacks that are *neither de jure* nor *de facto* organs of a State, but its behaviour is incited by the authorities of a State. In this sense, any armed or cyber attack by non-State actors against another State would be attributed to a State if such State later expressed support to them. However, this support must be more than mere endorsement or tacit approval.

The host State holds responsibility to exercise due diligence when taking the necessary and reasonable measures to stop attacks, such as disabling internet access. However, according to the *effective control test*, those cyber attacks of large scale and effects that are originated from computers located in certain States without any State involvement, cannot be attributed to the host State. in other words ,the mere breach of a State's obligation to not allow knowingly to use its territory or cyber infrastructure by non-State actors or hackers, cannot be enough to attribute such attacks to the host State to justify the right of self-defence. Nevertheless, deliberate failures by host State to act according to the duty of due diligence or unwillingness to take measures to stop attacks by non-State actors from its

territory, in extreme situations, can justify the use of force in the right of self-defence by the victim State directly against non-State actors.

EIGHTH. According to the strict approach on the right of self-defence, over the years, the prevailing view to exercise the inherent right of self-defence was limited to inter-State relations. In this regard, International Law authorizes resorting to the right of self-defence to repel direct armed attacks by State or indirect armed attacks when a State is *substantially involved* in such attacks by sending irregular armed groups or through effective control of the attack. However, in the last decades, new threats have appeared. They are the non-State actors and now have a high ability to carry out actions with catastrophic results that have changed the traditional and restrictive interpretation of the right of self-defence.

Both the UNSC Resolutions 1368 and 1373 in 2001 and recent State practice indicates that the international community tends to accept the right of self-defence against non-State actors even without substantial involvement of a State. Then, in spite of some doubts among some legal doctrine on the application of the right of self-defence against non-State actors, based on the State practice and approval of the majority of individual and collective doctrine, nowadays, resorting to such right of self-defence is acceptable against armed attacks by non-State actors, even without substantial involvement of host States, at least in front of those groups involved in terrorist operations.

In this sense, States can resort to the right of self-defence against non-State actors when such attacks are launched from a space beyond the sovereignty of any State or, in critical cases, when the attacks are originated from the territory of other States by non-State actors where such States are unwilling or unable to exercise territorial control over them. However, identifying, the willingness or unwillingness of host States is not easy. Therefore, in the context of cyber attacks by non-State actors, attacks with sufficient scale and effects can constitute an armed attack even if it is not attributed to a State. Nevertheless, resorting to the right of self-defence against cyber attacks by non-State actors is limited to some cases where the purposes of such attacks are against the political or national security of another State that violates its sovereignty. In this sense, all internet fraud, identity theft and intellectual property piracy can be cybercrimes, not cyber attacks.

NINTH. In general, an act of the use of force must be of sufficient gravity to carry out an armed attack to justify the exercise of the right of self-defence. However, in a particular situation, according to the *accumulation of events theory*, minor armed acts can constitute an armed attack if during a period of time an accumulation of acts, by one State or non-State actors against the same target in one case, reaches the level of graveness of an armed attack. This approach, explicitly and implicitly, appears to be accepted by the ICJ and the majority of the doctrine; nevertheless, to avoid any abuse of the right of self-defence, there is a great challenge to account how much or how many minor attacks are required to constitute an armed attack. Obviously, nowadays, because of the growing terrorist attacks, States are willing to accept this theory and allow the exercise of the right of self-defence to cope with these new threats. The *accumulation of events approach* is also applicable to confront the series of cyber attacks that are below the level of an armed attack when they accumulatively amount to an armed attack. In order for a cyber attacks to amount to an armed attack, such cyber attacks can be combined with other armed forces, such as military; therefore, it is not necessary to account for cyber attacks individually.

TENTH. In conformity with International Law, some essential requirements must be met to exercise the right of self-defence. One of these requirements is the *necessity* which, along with proportionality, are the two sides of the same coin and both are strictly linked together, provided that any reaction in the right of self-defence must be necessary and proportional to the objective which is supposed to achieve. According to International Law, clear and absolute necessity must exist to justify the right of self-defence. Necessity requirement means that the use of force is the only possibility to repel an armed attack and there is no other practicable lawful alternative to stop the attack. In this sense, self-defence has to be used for defensive purposes only and must not be applied to achieve other purposes, such as retaliatory, deterrent or punitive.

In order to assess the necessity criteria against non-State actors that are launching attacks from the territory of another State, it is accepted by unanimity that the necessity requirement depends primarily on the reaction of the host State. In this sense, in extreme situations, prior to resorting to the exercise of the right of self-defence, the victim State must request the host State to overwhelm non-State actors. Alternatively, the victim State

might cooperate with the host State to repress such groups or may require the consent of the host State to conduct extraterritorial measures against non-State actors. Then, there is *prioritization of consent and cooperation* of the host State before resorting to the right of self-defence against non-State actors in the territory of another State.

In this context, *unable* and *unwilling* test can be activated to make noticeable the necessity requirement in the right of self-defence against non-State actors while these groups use the State sovereignty as shield to deter reactions from the victim State. Therefore, in accordance with the necessity criteria, if the host State is *unable or unwilling* to conduct any effective action against an armed attack originated in its territory by non-State actors, in extreme situations, a victim State has the right to use the force in the right of self-defence directly against non-State actors. It is noticeable that the *unwilling* and *unable* test cannot provide high burden to attribute an armed attack to the host State to justify the use of force in the right of self-defence against the host State.

Therefore, in the context of cyber operations, the forcible reaction must be a mean of last resort; hence, if passive cyber defence is adequate to thwart the cyber attack, or if there is an opportunity to begin helpful negotiations, forceful defensive measures would be disallowed. Likewise, in order to meet the necessity requirement, the cyber attack must have hostile intentions and cannot be accidental.

Regarding the complex characteristics of cyber operations, the accomplishment of necessity requirement is very difficult, if not impossible, especially against non-State actors in the territory of another State; given the ease at which cyber attacks can now be conducted, such as by means of a computer, it is really difficult to prove the unwillingness of the host State to control or to prevent non-State actors from launching cyber attacks. Therefore, based on specific features of cyber operations, the necessity criteria depends on each circumstance that can be judged from the perspective of the victim State. However, this reasonable assessment of necessity does not mean that it opens the door to abuses of the right of self-defence. Nevertheless, it is noticeable that the right of self-defence would be unnecessary if the UNSC took appropriate measures to restore international peace and security.

ELEVENTH**.** Proportionality as a requirement to exercise the right of self-defence can be depicted as the essence of self-defence to restrict its exercise. In accordance with International Law, any reaction in the right of self-defence must be proportionate to the armed attack, neither unreasonable nor excessive. In conformity with the interpretation of proportionality known as double proportionality, firstly, according to the ICJ, the use of force in the right of self-defence would depend on the size and scope of the armed attack which amount of force in self-defence would be determined through the account of scale of the whole operations of attacks. Secondly, the response must be proportionate to repel the attack and aim at restoring the possible damages to the *status quo ante,* previous to the attack. This point of view is supported by most scholars and some ICJ judges.

Therefore, in general, based on the proportionality criteria, it is accepted that: i) the kind of means in defensive action do not necessarily have to be the same means which the attacker used, ii) a proportionate action have to be limited to the defensive purpose and not exceed the amount of force that is necessary to repel the armed attack, and iii) in order to use force in the right of self-defence to repel an armed attack in the border area, the defending State may temporarily penetrate into the territory of another State, but it must end at the moment when the aggressor stops using the armed force.

Traditionally, the exercise of the right of self-defence must not be remoteness from the origin of the armed attack, because it would violate the proportionality (and necessity) requirements. However, nowadays, this approach is very difficult to sustain in light of unique characteristics of cyber attacks where there are no geographical limitations in the origin and effects of the attacks. Furthermore, in the anticipatory self-defence, the proportionate reaction is not limited to repel the armed attack and must be applied to revert imminent armed attacks. However, the amount of physical and economic consequences should not be bigger than the harm expected from such armed attacks.

According to the International Law, if the victim State met both the necessary and immediacy requirements to justify the right of self-defence but it did not follow the criteria of proportionality, its reaction would not be as serious as an act of aggression; in this case, the violation of the principle of the prohibition of the use of force cannot be equated with who just acted exceeding (no proportionality) in self-defence.

The international practice indicates some general principles to determine proportionate response to confront non-State actors. First, the essential objective of the effects of self-defence effects is to repel the attack and prevent further armed attacks from succeeding; then, the exercise of the right of self-defence must repel an ongoing armed attack and prevent future situations to conduct an armed attack by weakening non-State actors. Second, recent State practice shows that States usually support the *quantitative concept* of proportionality. Third, however, in some cases the response in the right of self-defence may be more intense rather than an initial armed attack to weaken non-State actors. Forth, the aim of self-defence is to end ongoing damages; hence, proportionality is defined to achieve this legitimate aim. Fifth, nowadays, there is no geographical limitation to respond in self-defence and any reaction can target different bases of non-State actors even far-away of circumstance. Sixth, there is a general principle of International Law that asserts that any response on self-defence must only target non-State actors in the territory of anoother State. And seventh, in light of proportionality, any operation in self-defence against non-State actors must avoid civilian suffering.

In the context of cyber operations, proportionality in a cyber attack implies that the degree of cyber force employed is limited in magnitude to the intensity and duration to what is reasonably necessary to counter the attack. Then, any response must be proportionate in light of its objective and damages or causalities that will result from it.

According to the prevailing view on proportionate criteria, States in self-defence have the right to use kinetic force in response to a cyber attack if the attacker is invulnerable to cyber attacks; there is no reason to deprive kinetic operations to repel the attacker. But regarding the nature of cyber space, applying proportionate criteria in the exercise of the right of self-defence is very difficult, if not impossible. Some of these difficulties derive from assessing how much force employed in cyber terms it is proportionate to counter a cyber attack when the effects of such attack, in certain cases, are so devastating that it is not possible to account for a proportionate response. Additionally, there exists the problematic of the uncontrollable cyber attacks or the inability of the defensive State, in the right of self-defence, to limit its cyber reactions to the intended target. Also, regarding the complicated nature of cyber operation, the prediction of effects of the imminent attack is

too hard; hence, exerting proportionate and necessity criteria in the field of anticipatory self-defence is very difficult.

In summary, as in the necessity requirement, due to the immediate nature of the response, proportionality conditions must be assessed based on the circumstances of every particular case.

TWELFTH. Immediacy is a requirement to justify the right of self-defence in International Law. According to this criterion, the response to an armed attack must be immediate. This requirement has close relation with the necessity requirement because if there is not immediacy, there is not necessity to react. In this sense, defensive action must be current and any delay to react against an armed attack would turn the use of force in the right of self-defence into an armed retaliation, which is prohibited under article 2(4) of the UN Charter. Hence, there must be temporal proximity between the armed attack and response. Nevertheless, due to the characteristics of cyber operations, there may be a time-lag of day, weeks and even months between the beginning of the cyber attack and the effects of such attack. That is why, it is advisable to have a flexible and extensive view on the immediacy criteria regarding the cyber attack. In this context, immediacy does not mean *instantaneously.* It can be applied flexibly but there must be no undue time-lag between the cyber attack and the reaction in the right of self-defence. Therefore, although International Law does not authorize States to act in the right of self-defence *a posteriori*, the nature of cyber space causes that, in some circumstances, such right can be justified *a posterior* against cyber attacks.

THIRTEENTH**.** The requirement of immediacy should not be confused with the imminence in the context of anticipatory self-defence. According to International Law, *imminent* threat is covered by article 51 of the UN Charter (and general International Law), but the response to other latent threats that are not *imminent* is under the authority of the UNSC to use force to maintain international peace and security. Although, all preventive and pre-emptive or anticipatory self-defence refer to the use of force prior to the occurrence of an armed attack, anticipatory is used when a threat is *imminent,* while, preventive and pre-emptive occur when the threat is latent but not *imminent*.

After analysing different documents that go from the *High-level Panel on Threats, Challenges and Change* of 2004 to the *Tallinn Manual 2.0* rules of 2017 and verifying the tendency of many State to accept explicitly to use force against imminent attacks, it seems that the international community has admitted that the resort to the right of self-defence only against a consummated attacks is not realistic to cope with cyber attacks, especially with the increasingly complex technology. Therefore, the use of force in the anticipatory self-defence is justifiable when an armed attack is *imminent*. However, the pre-emptive self-defence *versus* the latent threats is only maintained by some doctrine.

According to the anticipatory self-defence, States that act in self-defence do not necessarily have to wait for an armed attack to occur. Hence, in the context of cyber operations, a State is not required to be inactive until the cyber attack takes place. If a State is aware that its computer systems will be under the effects of a cyber attack, it can take passive or active cyber defence measures to thwart the threat. In the case that all these measures failed, it could resort to the anticipatory self-defence.

In the context of cyber operations, assessing the *imminent* threat in cyber space is more difficult than in the kinetic field. In cyber space, there are some challenges to apply temporal criteria, because normally there is not any warning to indicate that the attack is *imminent* and the interval between the launching of the attack and the occurrence of its effects can be just a matter of seconds. Thus, meeting the requirement of *imminent* in the anticipatory self-defence is difficult, if not impossible. In fact, the identification of the *imminent* threat of cyber attacks are based on the assessment by the target State on its evidence that such attack is *imminent* and that it will give rise to harm vital infrastructures and/or loses of human life. In this regard, in order to cope with such a modern technological threat in cyber space, some scholars reject the strict temporal analysis and refer to the *last feasible window of opportunity* standard. Thus, States have the right to use anticipatory self-defence against cyber or kinetic armed attacks when the attacker will reasonably launch the attack and the victim State will lose its opportunity to defend itself effectively, unless it reacts in self-defence.

However, the *last feasible window of opportunity* to use force in anticipatory self-defence must not be interpreted as the use of preventive strikes against another State or non-State actors who lack either the means or of the intention to carry out an armed attack. In this sense, if the hostile State barely has the capability to launch a cyber attack, even with possibly devastating results, the potential victim State will not be able to resort to the right of self-defence and any use of force would fall under an unlawful preventive self-defence. In this regard, all non-imminent cyber threats must be reported to the UNSC. Therefore, any preventive use of force against an armed attack is unlawful.

Some of the greatest technical challenges are found in the difficulties to identify the attacker and the amount of time needed to attribute the attack, intention, nature and effects of the threat to choose the most suitable type of reaction according to the necessity and proportionality criteria, along with a reasonable degree of certainty. Nowadays, geopolitical and technological developments impose additional pressure on the legal framework in the anticipatory self-defence when non-State actors bent on conducting spectacular attacks where the traditional military signals forecasting an imminent attack would often be *absent* regarding the speed and complexity of cyber attacks. As a result, in the context of cyber operations and in consideration to the technical challenges of cyber space, the application of the requirements of self-defence is very difficult and must be examined case-by-case. In most circumstances, identifying the conditions to resort to the right of self-defence would be based on the reasonable assessment of the defender State that, in practice, can open the door to abuses of such right.

FOURTEENTH, the right of self-defence is an exception to the prohibition of the use of force in International Law. In fact, with the recognition of the individual or collective right of self-defence under article 51 of the UN Charter, the international community accepts implicitly the role of the States to maintain international peace and security when they resort to such right. In practice, collective security system, envisaged in the San Francisco Conference which has not worked during the cold war due to the right of veto from UNSC permanent members, has been replaced by a system of collective self-defence. This is one of the major changes in the prognostics of the UN Charter.

Despite the difficulties to adapt the right of self-defence to cover new threats through *cyber space*, especially by *non-State actors*, the international community attempted to cope with this challenges with a flexible approach in the use of force in self-defence which, in principle, is contrary to the essence of the right of self-defence provided that the restrictive view has always been prevailing.

In effect, during the last decades, the exceptions to the prohibition of the use of force have evolved significantly to a less restrictive view. On one side, the UNSC authorization for the use of force under Chapter VII of the UN Charter has been relaxed from the strict prior authorization to the *a posteriori* consent (for instance, the UNSC Resolution 1483 of 22 May 2003 related to Iraq). What is more, there lies the possibility that some recent doctrine opens the door to accept the implicit permission of the UNSC (acquiescence), when nobody protests in particular powerful States against acts of use of force. (especially when they are taken under the responsibility to protect).

On the other side, the conception of the right of self-defence has changed due to two main factors: first, the appearance of the phenomena of terrorist acts carried out by non-State actors; and second, the emergence of new ways of threat or use of force into international arena, especially through cyber space, and the fact that developed States are more vulnerable to cyber operations than developing States.

As a result of these factors, the use of force under the right of self-defence has evolved towards a broader view. In this sense, first, the right of self-defence has changed from being only applicable against ongoing attacks to a more flexible response to confront imminent attacks (anticipatory) and the possibility to react *a posteriori* against cyber operations; and secondly, has brought about the possibility of using force under the right of self-defence against non-State actors. Therefore, the international community has reached a broader approach by confronting the origin of the armed attacks with the inclusion of non-State actors, and in front of the immediacy requirement in relation to the temporal dimension.

FIFTEENTH. Regarding the nature of cyberspace, which is caused by the complexity and novelty of digital attacks and obscuring incidents, it is necessary to consider international interconnections in cyber space. In other words, the international community must increase cooperation and informational exchange in the context of cyber security and

cybercrime, because only with a joint and coordinated effort it is effectively possible to respond to the threats originating from cyber space.

Until now, cyber technologies with complex characteristics have caused serious challenges to the State's sovereignty and to the maintaining of international peace and security, given the ambiguities in the current rules of International Law to cope with the new threats raised by such technologies. Hence, the international community must find legal solutions to deal with these new challenges, particularly, with cyber attacks.

International cooperation is necessary to avoid the new ICT being used, not only for the benefit of a few economic agents of the industrialized countries, but also as a key factor in finding solutions, as broad as possible, to international, economic, social, cultural and humanitarian problems, under the conditions of freedom.

In this regard, all governments and international organizations, in good faith, should negotiate closely and directly, and research in order to achieve a comprehensive and long lasting settlement based on the norms and principles of International Law. In this respect, governments ought to work on a set of behavioural norms addressing State-to-State and State-to-non-State actor's behaviour in cyberspace. In order to combat threats of cyber operations by States or non-State actors, States have to seek ways to better enhance international cooperation through the exchange of practices and promote responsible and active cyber policies at national and international level. In other words, governments have to note down in their agendas the duty to draft and enforce national and international regulations based on confidence, transparency and security by building measures that would help control malicious cyber operations, especially by non-State actors. A single State cannot cope with the new challenges of cyber space on its own.

Therefore, all cyber challenges require that the international community attempts to reach a consensus on the legal alternative rules to provide appropriate solutions to cope with the new threats that arise through the cyber space.

SIXTEENTH. To provide solutions to cyber challenges, there are different options. One possible solution would be to review International Law, especially the UN Charter provisions, particularly, article 2(4), related to the principles of the prohibition of the

threat or use of force and article 51 on the right of self-defence. The review should seek to give answer to new threats by clarifying the current rules; for instance, recognizing the anticipatory right of self-defence against non-State actors. While this option is the most suitable one, it seems almost impossible because the great powers, particularly the permanent members of the UNSC, will not give in to clarify rules in the field of the use of force, since the lack of rules and ambiguities allow them to better pursue their national interests.

Another option is to provide a general treaty on cyber space activities. However, it seems that the necessary consensus for the adoption of specific norms adapted to the characteristics of cyber space would be difficult. The failure of the UN, especially of the GGE, to achieve consensus on its final report and the uncertain future of such Groups, shows that States may mainly move towards regional or bilateral agreements, in very specific fields, such as the COE Convention on cybercrime of 2001. Thus, regarding precedent experience, gaining a new global consensus to accept a general treaty does not look feasible.

Due to the difficulties when finding a consensus to carry out the precedent options, the choice of international community may go in different directions. In this sense, one option is that the ICJ provided more clear interpretations around the principle of the prohibition of the threat or use of force and the right of self-defence. These new interpretations must be adapted to the new reality to overcome cyber space challenges in relation to the use of force.

The other alternative solution is the application by analogy of the pre-existing rules of International Law to the cyber space, particularly in the field of the use of force. This way, new practices can arise among States in international community, in accordance with the existing principles and norms of International Law. The generalized acceptance of these new practices can facilitate the consolidation of new rules of general International Law. At least until now, it seems that the practice has been in this direction. However, this option presents some difficulties. On one side, sometimes they must cope with the contrary and restrictive view of precedent jurisprudence on the right of self-defence. On the other side,

normally, this solution does not give precise answers to different issues involved in the exercise of the right of self-defence (necessity, proportionality or immediacy). In fact, this approach, which facilitates the ambiguity of the rules, favours the powerful States' interests. Thus, to our understanding, the ICJ interpretations, that are more adapted to the new reality, may be the most appropriate and feasible solutions to overcome cyber space challenges.

DOCUMENTS

A. International treaties

- The Hague Convention (I) for the Pacific Settlement of International Disputes, 29 July 1899.

- The Hague Convention (I) for the Pacific Settlement of International Disputes, 18 October 1907.

-The Hague Convention (II) on the Limitation of the Employment of Force for the Recovery of Contract Debts, 18 October 1907.

- The Hague Convention (III) on the Opening of Hostilities, 18 October 1907.

- The Covenant of the League of Nations, 28 April 1919.

- Geneva Protocol for the Pacific Settlement of International Disputes, 2 October 1924.

- The General Treaty for Renunciation of War (Kellogg-Briand Pact), 27 August 1928.

- Charter of the United Nations, 26 June 1945.

- The North Atlantic Treaty Organization, 4 April 1949.

- Protocol Additional to the Geneva Conventions of 12 august 1949, relating to the - Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.

- Treaty on the Non-Proliferation of Nuclear Weapons (NPT), 1 July 1968.

- Vienna Convention on the Law of Treaties, 22 May 1969.

-The United Nations Convention on the Law of Sea, 10 December 1982.

- Consolidated version of the Treaty on European Union, 7 February 1992.

- Rome Statute of the International Criminal Court (ICC), 17 July 1998.

- Convention on Cybercrime, 23 November 2001.

- African Union Non-Aggression and Common Defence Pact, 31 January 2005.

- Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 16 June 2009.

B. **International Jurisprudence**

1. *ICJ*

- *Corfu Channel case* (United Kingdom *v.* Albania), judgment of 9 April 1949, *ICJ Reports 1949*, p. 4.

- *Legal consequences for States of the continued presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (197*0), advisory opinion of 21 June 1971, *ICJ Reports* 1971, p. 16.

- *Western Sahara*, advisory opinion of 16 October 1975, *ICJ Reports 1975*, p. 12.

- *Case concerning United States diplomatic and consular staff in Tehran (*United States *v.* Iran), judgment of 24 May 1980, *ICJ Reports 1980,* p. 3.

- *Military and paramilitary activities in and against Nicaragua* (Nicaragua *v.* United States of America*)*, judgment of 27 June 1986, *ICJ Reports* 1986, p. 14.

- *Legality of the threat or use of nuclear weapons,* advisory opinion, of 8 July 1996, *ICJ Reports 1996*, p. 226.

- *Fisheries Jurisdiction Case* (Spain *v.* Canada), judgment of 4 December 1998, *ICJ Reports 1998,* p. 432.

- *Case concerning land and maritime boundary between Cameroon and Nigeria* (Cameroon *v.* Nigeria: Equatorial Guinea intervening), judgment of 10 October 2002, *ICJ Reports* 2002, p. 303.

- *Case concerning Oil Platforms* (Islamic Republic of Iran *v.* United States of America), judgment of 6 November 2003, *ICJ Reports 2003*, p. 161.

- *Legal consequences of the construction of a wall in the occupied Palestinian territory,* advisory opinion of 9 July 2004, *ICJ Reports 2004*, p. 136.

- *Case concerning armed activities on the territory of the Congo (*Democratic Republic of Congo *v.* Uganda*),* judgment of 19 December 2005, *ICJ Reports 2005*, p. 168.

- *Case concerning application of the Convention on the prevention and punishment of the crime of genocide*, (Bosnia and Herzegovina *v.* Serbia and Montenegro), judgment of 26 February 2007, *ICJ Reports 2007*, p. 43.

-Accordance with International Law of the unilateral declaration of independence in respect of Kosovo, advisory opinion, of 22 July 2010, *ICJ Report* 2010, p. 16.

- *Certain activities carried out by Nicaragua in the border area (Costa Rica v. Nicaragua) and construction of a road in Costa Rica along the San Juan river* (Nicaragua v. Costa Rica), judgment of 16 December 2015, *ICJ Reports 2015*, p. 665.

2. *Other jurisprudence*

- US SUPREME COURT, *The Caroline v. United States*, 11, *US 7 Cranch,* 1813, p. 496.

- ARBITRAL TRIBUNAL, *Naulilaa Incident*, (Portugal *v.* Germany), award of 31 July 1928, *RIAA,* II, p. 1026.

- INTERNATIONAL MILITARY TRIBUNAL (Nuremberg), judgment of 1 October 1946, reproduced in *AJIL*, 41, 1947, p. 172.

- US MILITARY TRIBUNAL V, *High command trial,* United States of America *vs.* Wilhelm von Leeb *et al*., judgment of 27 October 1948, *Trials of War Criminals Before the Nuremberg Military Tribunals*, vol. IX, p. 462.

- ICTY, APPEALS CHAMBER, *Presocutor v. Tadic*, case No IT-94-1-A, judgment, 15 July 1999.

- ECHR, *Case of Ilaşcu and others v. Moldova and Russia*, application No 48787/99, judgment of 8 July 2004, *Reports of Judgments and Decisions*, VII, p. 179.

- ERITREA ETHIOPIA CLAIMS COMMISSION, partial award, *jus ad bellum*, Ethiopia's Claims 1-8, (Ethiopia *v.* Eritrea), award of 19 December 2005*, RIAA*, XXVI, p. 457.

- ARBITRAL TRIBUNAL, *Award in the arbitration regarding the delimitation of the maritime boundary between Guyana and Suriname*, award of 17 September 2007, *RIAA*, XXX, p. 1.

C. **International Organizations documents**

1. *UN documents*

a) *UNGA*

i) Resolutions

- Resolution 4/290 on "Essentials of peace", 1 December 1949.

-Resolution 377A (V) on "Uniting for peace", 3 November 1950.

- Resolution 1001(ES-I) on Middle East, 7 November 1956.

- Resolution 1514 (XV) on "Declaration on the granting of independence to Colonial Countries and peoples", 14 December 1960.

- Resolution 1541 (XV) on "Principles which should guide Members in determining whether or not an obligation exists to transmit the information called for under Article 73e of the Charter", 15 December 1960.

- Resolution 1991 (XVIII) on “Question of equitable representation on the Security Council and the Economic and Social Council”, 17 December 1963.

- Resolution 2131 (XX) on “Declaration on the inadmissibility of intervention in the domestic affairs of States and the protection of their independence and sovereignty”, 21 December 1965.

-Resolution 2160 (XXI) on “Strict observance of the prohibition of the threat or use of force in international relations, and of the right of peoples to self-determination”, 30 November 1966.

- Resolution 2625(XXV) on “Declaration on principles of International Law concerning friendly relations and cooperation among States in accordance with the Charter of the United Nations”, 24 October 1970.

- Resolution 2734 (XXV) on “Declaration on the strengthening of international security”, of 16 December 1970.

- Resolution 3314 (XXIX) on “Definition of aggression”, 14 December 1974.

- Resolution 35/227 A on “Question of Namibia”, 6 March 1981.

- Resolution 36/27 on “Armed Israeli aggression against the Iraq nuclear installations and its grave consequences for the established international system concerning the peaceful uses of nuclear energy, the non-proliferation of nuclear weapons and international peace and security”, 13 November 1981.

- Resolution 36/103 “Declaration on the inadmissibility of and interference in the internal affairs of States“, 9 December 1981.

- Resolution 37/18 on “Armed Israeli aggression against the Iraqi nuclear installations and its grave consequences for the established international system concerning the peaceful uses of nuclear energy, the non-proliferation of nuclear weapons and international peace and security”, 16 November 1982.

- Resolution 38/9 on “Armed Israeli aggression against the Iraqi nuclear installations and its grave consequences for the established international system concerning the peaceful uses of nuclear energy, the non-proliferation of nuclear weapons and international peace and security”, 10 November 1983.

- Resolution 39/14 on “Armed Israeli aggression against the Iraqi nuclear installations and its grave consequences for the established international system concerning the peaceful uses of nuclear energy, the non-proliferation of nuclear weapons and international peace and security”, 16 November 1984.

- Resolution 40/6 on “Armed Israeli aggression against the Iraqi nuclear installations and its grave consequences for the established international system concerning the peaceful

uses of nuclear energy, the non-proliferation of nuclear weapons and international peace and security", 1 November 1985.

- Resolutions 40/32 on the prevention of crime and the treatment of offenders, 29 November 1985.

- Resolution 41/12 on "Armed Israeli aggression against the Iraqi nuclear installations and its grave consequences for the established international system concerning the peaceful uses of nuclear energy, the non-proliferation of nuclear weapons and international peace and security", 29 October 1986.

- Resolution 42/22 on "Declaration on the enhancement of the effectiveness of the principle of refraining from the threat or use of force in international relations", 18 November 1987.

- Resolution 42/52 on "Efforts and measures for securing the implementation by States and the enjoyment by youth of human rights in conditions of peace, particularly the right to education and to work", 30 November 1987.

- Resolutions 44/72 on "Crime prevention and criminal justice", 8 December 1989.

- Resolution 45/121 on the prevention of crime and the treatment of offenders, 14 December 1990.

- Resolution 50/172 on "Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes", 27 February 1996.

- Resolution 53/70 on "Developments in the field of information and telecommunications in the context of international security", 4 December 1998.

- Resolution 54/49 on "Developments in the field of information and telecommunications in the context of international security", 1 December 1999.

- Resolution 55/28 on "Developments in the field of information and telecommunications in the context of international security", 20 November 2000.

- Resolution 56/19 on "Developments in the field of information and telecommunications in the context of international security", 29 November 2001.

- Resolution 56/152 on "Respect for the purposes and principles contained in the Charter of the UN to achieve international cooperation in promoting and encouraging respect for human rights and for fundamental freedoms and in solving international problems of a humanitarian character", 19 December 2001.

- Resolution 56/1 on "Condemnation of terrorist attacks in the United States of America", 12 September 2001.

- Resolution 57/53 on "Developments in the field of information and telecommunications in the context of international security", 22 November 2002.

- Resolution 57/239 on “Creation of a global culture of cybersecurity”, 20 December 2002.

- Resolution 58/32 “Developments in the field of information and telecommunications in the context of international security”, 8 December 2003.

- Resolution A/RES/ES-10/14 on “Illegal Israeli actions in occupied East Jerusalem and the rest of the occupied Palestinian territory, 8 December 2003.

- Resolution 58/199 on “Creation of a global culture of cybersecurity and the protection of critical information infrastructures”, 23 December 2003.

- Resolution 59/61 on “Developments in the field of information and telecommunications in the context of international security”, 3 December 2004.

- Resolution A/RES/60/1 on “World summit outcome”, 16 September 2005.

- Resolution 60/45 on “Developments in the field of information and telecommunications in the context of international security”, 8 December 2005.

- Resolution 61/54 on “Developments in the field of information and telecommunications in the context of international security”, 6 December 2006.

- Resolution 62/17 on “Developments in the field of information and telecommunications in the context of international security”, 5 December 2007.

- Resolution 63/37 on “Developments in the field of information and telecommunications in the context of international security”, 2 December 2008.

- Resolution 64/25 on “Developments in the field of information and telecommunications in the context of international security”, 2 December 2009.

- Resolution 64/211 on “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures”, 21 December 2009.

- Resolution 65/41 on “Developments in the field of information and telecommunications in the context of international security”, 8 December 2010.

- Resolution 66/24 on “Developments in the field of information and telecommunications in the context of international security”, 2 December 2011.

- Resolution 67/27 on “Developments in the field of information and telecommunications in the context of international security”, 3 December 2012.

- Resolution 68/243 on “Developments in the field of information and telecommunications in the context of international security”, 27 December 2013.

- Resolution 69/28 on “Developments in the field of information and telecommunications in the context of international security”, 2 December 2014.

- Resolution 70/237 on "Developments in the field of information and telecommunications in the context of international security", 23 December 2015.

- Resolution on 71/28 "Developments in the field of information and telecommunications in the context of international security", 5 December 2016.

ii) Other documents

- Doc. A/2211, *Official Records of the UN General Assembly, Seventh Session, Annexes*, agenda item 54, 3 October 1952.

- Doc. A/8018, *Report of Special Committee on Principles of International Law concerning friendly relations and cooperation among States*, Official Records of the General Assembly, 25th Session, Supplement No. 18, 1 May 1970.

- Doc. A/41/41, *Report of the Special Committee on enhancing the effectiveness of the principle of non-use of force in international relation meeting*, UNGA, 41st Session, supplement No. 41 13 March 1986.

- Doc. A/C.1/53/3 on "Role of science and technology in the context of international security, disarmament and other related fields", 30 September 1998.

- Doc. A/54/213 on "Developments in the field of information and telecommunications in the context of international security", 10 August 1999.

- Doc. A/59/565, *Note [transmitting report of the High-level Panel on Threats, Challenges and Change, entitled "A more secure world: our shared responsibility"],* 2 December 2004.

- Doc. A/59/2005, Secretary-General's report "In larger freedom: towards development, security and human rights for all", 21 March 2005.

- Doc. A/65/201, on "Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security", 30 July 2010.

- Doc. A/66/152 on "Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General", 15 July 2011.

- Doc. A/66/359 "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", 14 September 2011.

- Doc. A/68/98 on "Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security", 24 June 2013.

- Doc. A/68/156 on "Developments in the field of information and telecommunications in the context of international security", 16 July 2013.

- Doc. A/69/112 on “Developments in the field of information and telecommunications in the context of international security”, 30 June 2014.

- Doc. A/70/172 on “Developments in the field of information and telecommunications in the context of international security”, 22 July 2015.

- Doc. A/70/174 on “Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security”, 22 July 2015.

- Doc. A/71/172 on “Developments in the field of information and telecommunications in the context of international security”, 19 July 2016.

- Doc. A/72/315 on “Developments in the field of information and telecommunications in the context of international security”, 11 August 2017.

b) *UNSC*

i) Resolutions

- Resolution 188 on “Complaint by Yemen”, 9 April 1964.

- Resolution 228 on “The Palestine Question”, 25 November 1966.

- Resolution 248 on the Middle East, 24 March 1968.

- Resolution 256 on the Middle East, 16 August 1968.

- Resolution 262 on the Middle East, 31 December of 1968.

- Resolution 265 on Middle East, 1 April 1969.

- Resolution 270 on Middle East, 26 August 1969.

- Resolution 395 on “Complaint by Greece against Turkey”, 25 August 1976.

- Resolution 405 on Benin, 14 April 1977.

- Resolution 419 on Benin, 24 November 1977.

- Resolution 450 on the Israel, Lebanon, Middle East, 14 June 1979.

- Resolution 487on Iraq-Israel, 19 June 1981.

- Resolution 502 on Falkland Islands (Malvinas), 3 April 1982.

- Resolutions 509 on the Israel, Lebanon, Middle East, 26 May 1982.

- Resolution 512 on Lebanon, 19 June 1982.

- Resolution 513 on Lebanon, 4 July 1982.

- Resolution 515 on Israel-Lebanon, 29 July 1982.

- Resolution 567 on Angola-South Africa, 20 June 1985.

- *Resolution 568 on Botswana-South Africa, 21 June 1985.*

- *Resolution 571 on Angola-South Africa, 20 September 1985.*

- Resolution 573 on Israel-Tunisia, 4 October 1985.

- Resolution 582 on situation between Islamic Republic of Iran-Iraq, 24 February 1986.

- Resolution 598 on Iraq-Islamic Republic of Iran, 20 July 1987.

- Resolution 611 on Middle East, 25 April 1988.

- Resolution 1154 on Iraq, 2 March 1998.

- Resolution 660 on Iraq-Kuwait, 2 August 1990.

- Resolution 661 on Iraq-Kuwait, 6 August 1990.

- Resolution 678 on Iraq-Kuwait, 29 November 1990

-Resolution S/23500 on "The responsibility of the Security Council in the maintenance of international peace and security", 31 January 1992.

- Resolution 811 on Angola, 12 March 1993.

- Resolution 823 on Angola, 30 April 1993.

- Resolution 834 on Angola, 1 June 1993.

- Resolution 851on Angola, 15 July 1993.

- Resolution 913 on Bosnia and Herzegovina, 22 April 1994.

- Resolution 1034 on Bosnia and Herzegovina, 21 December 1995.

- Resolution 1127 on Angola, 28 August 1996.

- Resolution 1071 on Liberia, 30 August 1996.

- Resolution 1154 on Iraq -Kuwait, 2 March 1998.

- Resolution 1189 on the international terrorism, 13 August 1998.

- Resolution 1237 on Angola, 7 May 1999.

- Resolution 1244 on the situation relating Kosovo, 10 June 1999.

- Resolution 1368 on "Threats to international peace and security caused by terrorist acts", 12 September 2001.

- Resolution 1373 on "Threats to international peace and security caused by terrorist acts", 28 September 2001.

- Resolution 1397 on the situation on the Middle East Palestine, 12 March 2002.

- Resolution 1441 on Iraq-Kuwait non-proliferation of weapons, 8 November 2002.

- Resolution 2249 on threats to international peace and security caused by terrorist acts, 20 November 2015.

ii) Other documents

- Doc. S/PV.1939, Security Council official records, 31st year, 1939th meeting, 9 July 1976.

- Doc. S/23500 on the responsibility of the Security Council in the maintenance of international peace and security, 31 January 1992.

- Doc. S/PV.3438 on the situation between Iraq-Kuwait, 15 October 1994.

- Doc. S/PV.3439 on the situation between Iraq-Kuwait, 17 October 1994.

- Doc. S/1998/780, letter from the Permanent representative of the United State of America to UN to address the Security Council, 20 August 1998.

- Doc. S/2001/946, letter from the Permanent Representative of the United States of America to the President of the Security Council, 7 October 2001.

- Doc. S/2001/947, letter from the Charge d'Affaires of the United Kingdom to the President of the Security Council, 7 October 2001

- Doc. S/2002/1012 on "Letter from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General", 12 September 2002.

- Doc. S/PV.5489 on "The situation in the Middle East", 14 July 2006.

- Doc. S/PV.5492 on "The situation in the Middle East", 20 July 2006.

- Doc. S/PV. 5493 on “The situation in the Middle East, including the Palestinian question”, 21 July 2006.

- Doc. S/2007/436, “Letter from the Chairman of the Security Council Committee established pursuant to Resolution 751 (1992) concerning Somalia addressed to the President of the Security Council”, 18 July 2007.

- Doc. S/2008/814, letter from the Permanent Representative of Israel to the UN, 24 December 2008.

- Doc. S/2008/816, letter from the Permanent Representative of Israel to the United Nations, 27 December 2008.

- Doc. S/PV.6060 on “The situation in the Middle East, including the Palestinian question”, 31 December 2008.

- Doc. S/PV.6061 on “The situation in the Middle East, including the Palestinian question”, 6 January 2009.

- Doc. S/2014/695, “Letter from the Permanent Representative of the United Stated of America to the United Nations addressed to the Secretary-General”, 23 September 2014.

- Doc. S/2015.221, letter from the Chargé d’affaires, a.i. and the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council, 31 March 2015.

- Doc. S/2015/563, letter from the Chargé d’affaires, a.i. and the Permanent Mission of Turkey to the United Nations addressed to the President of the Security Council, 24 July 2015.

- Doc. S/2015/693, letter from the Permanent Representative of Australia to the United Nations addressed to the President of the Security Council, 9 September 2015

- Doc. S/2015/719, letters from the Permanent Representative of the Syrian Arab Republic to the United Nations were addressed to the Secretary General and the President of the Security Council, 21 September 2015.

- Doc S/PV.7565 on “Threats to international peace and security caused by terrorist acts”, 20 November 2015.

c) *International Law Commission*

- "State responsibility", Documents of the thirty-second session, *Yearbook of ILC*, vol. II, part 1, 1980, p. 13-130.

- "State responsibility", Report of the Commission to the General Assembly on the work of its thirty-second session, *Yearbook of ILC*, vol. ll, part 2, 1980, p. 26-62.

- "Draft code of offences against the peace and security of mankind", Documents of the thirty-seventh session, *Yearbook of ILC,* vol. II, part 1, 1985, p. 63-86.

- "Draft Code of crimes against peace and security of mankind", Summary records of the meetings of the forty-first session, *Yearbook of ILC,* vol. I, 1989.

- "Draft Code of crimes against the peace and security of mankind", Report of the Commission to the General Assembly on the work of its forty-first session, *Yearbook of ILC*, vol. II, part 2, 1989, p. 50-70.

- "Draft code of crimes against peace and security Mankind", Summary records of the meetings of the forty-third session, *Yearbook of ILC*, vol. I, 1991.

- "Draft articles on State responsibility", *Yearbook of ILC*, vol. II, part 2, 1996, p. 57-65.

- *Draft articles on State Responsibility with commentaries thereto adopted by the International Law Commission on First Reading*, January 1997.

- *First Report on Diplomatic Protection*, 7th March 2000, UN, Doc. A/CN.4/506, p. 206-246.

- "Draft articles on responsibility of States for internationally wrongful acts, with commentaries", *Yearbook of ILC*, vol. ll, part 2, 2001, p. 31-143.

d) *Other UN documents*

UNCIO, *Documents of the United Nations Conference on International Organization,* Dumbarton Oaks proposals comments and proposed amendments, vol. III, San Francisco 1945.

- UNCIO, *Documents of the United Nations Conference on International Organization,* The Dumbarton Oaks Proposal for the Establishment of a General International Organization, vol. IV, San Francisco 1945.

- UNCIO, *Documents of the United Nations Conference on International Organization*, Commission I, General Provisions, vol. VI, San Francisco 1945.

- UNCIO, *Documents of the United Nations Conference on International Organization,* Commission III, Security Council, vol. XI, San Francisco 1945.

- Message of the Secretary-General to the International Conference on United Nations reform (delivered by Mr. Edward Mortimer, Director of Communications in the Office of the Secretary-General), Tehran, of 17 July 2005.

- Doc. A/60/937- S/2006/515, letter from the Permanent Representative of Israel to the United Nations, 12 July 2006.

- UN OFFICE ON DRUGS AND CRIME, *The use of the Internet for terrorist purposes,* 2012.

2. *Other International Organizations documents*

- NATO, *The Final Declaration of the Washington Summit*, of 23- 25 April 1999, available at https://www.nato.int/cps/en/natohq/official_texts_27433.htm, [visited on 24 April 2018] .

- COUNCIL OF THE EU, *Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001*, Doc. SN 140/01, available at https://www.consilium.europa.eu/media/20972/140en.pdf, [visited on 2 July 2018] .

- EU, *Proposal for a Council Framework Decision on attacks against information systems*, 19 April 2002, COM/2002/0173 final, *OJEU*, *203 E* , 27 August 2002.

- EU, Communication from the Commission to the Council and the European Parliament*, Critical infrastructure protect in the fight against terrorism*, Doc COM, 2004, 702 final, 20 October 2004, available at http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2004/0702/COM_COM(2004)0702_EN.pdf, [visited on 1 March 2018].

- COUNCIL OF THE EU, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJEU L 69*, 16 March 2005.

- OSCE PA, "Resolution on cyber security and cyber crime", *Astana Declaration of the OSCE Parliamentary Assembly and Resolutions adopted at the Seventeenth Annual Session*, 3 July 2008.
- EU, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *OJEU L* 345/75, 23rd December 2008.

- EU, INDEPENDENT INTERNATIONAL FACT-FINDING MISSION ON THE CONFLICT IN GEORGIA (IIFFMCG), *Report*, vol. I, II and III, September 2009, available at http://www.mpil.de/en/pub/publications/archive/independent_international_fact.cfm, [visited on 5 May 2018].

- OSCE PA, "Resolution on cyber crime", *Oslo Declaration of the OSCE Parliamentary Assembly and Resolutions adopted at the Nineteenth Annual Session*, 10 July 2010.

- NATO, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted by Heads of State and Government at the NATO Summit in Lisbon, 19 November 2010, available at https://www.nato.int/cps/en/natohq/official_texts_68580.htm, [visited on 22 May 2018].

- COE, *International and Multi-stakeholder co-operation on cross-border internet*, interim report of the Ad-hoc Advisory Group on Cross-border Internet to the steering Committee on the Media and New Communication Services incorporating analysis of proposal for international and multi-stakeholder co-operation on cross-border Internet, H/Inf, 2010, available at http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf, [visited on 12 June 2018].

- NATO, CZOSSECK C., *et al.* (eds.), *2012 4th International Conference on Cyber Conflict* (CYCON 2012), NATO CCD COE, 2012.

- EU, EUROPEAN COMMISSION and HREU, *Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* JOIN (2013) 1 final, 7 February 2013, available at https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf,]visited on 6 July 2017[.

- NATO, *Wales Summit Declaration*, 5 September 2014, available at https://www.nato.int/cps/en/natohq/official_texts_112964.htm, [visited on 6 June 2018].

- NATO's *Glossary of Terms and Definitions*, AAP-06, Edition 2017, available at file:///C:/Users/hamed/Downloads/AAP-06%202017%20(1).pdf, [visited on 22 June 2018].

- NATO-EU, *Joint Declaration; by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 8 July 2016, available at https://ccdcoe.org/eu-nato-relations-hand-hand-against-cyberattacks.html,, [visited on 4 May 2018].
- EU, Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJEU L 194*, 19 July 2016.

- EU, COUNCIL OF THE EU, *Council Conclusion on the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the NATO*, 6 December 2016, available at http://www.consilium.europa.eu/en/press/press-releases/2016/12/06/eu-nato-joint-declaration/, [visited on 8 June 2018].

- OSCE PA, *Minsk Declaration and Resolutions adopted by the OSCE Parliamentary Assembly at the Twenty-sixth Annual Session*, 9 July 2017.
- EU, COUNCIL OF THE EU, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),* 7 June 2017,

available at http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf,]visited on 8 June 2018[.
- NATO, CCDCOE, *Cyber definitions*, available at https://ccdcoe.org/cyber-definitions.html, [visited on 8 April 2018].

-OSCE PA, Lisbon Conference on *Digital Resilience of a Democratic State*, 8 May 2018, available at http://www.oscepa.org/news-a-media/press-releases/2853-protections-against-cyber-threats-must-build-trust-and-uphold-fundamental-freedoms-say-osce-parliamentarians-at-lisbon-conference, [visited on 8 June 2018].

-NATO, "Cyber defense", available at https://www.nato.int/cps/en/natohq/topics_78170.htm, [visited on 20 June 2018].

D. **Unilateral documents**

- US, *Foreign Relations of the United States: Diplomatic Papers, 1945, General: The United Nations,* vol. I, of 12 May 1945.

- US, *Excusive Order No. 13010*, "Critical Infrastructure Protection", 15 July 1996, 61(138), *Federal Register* 37347, 17 July 1996, available at https://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf, [visited on 3 April 2018].

- US, DoD, OFFICE OF GENERAL COUNSEL, *An Assessment of International Legal Issue in Information Operations*, Washington, May 1999, available at http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, [visited on 2 March 2018].

- RUSSIA FEDERATION, *Conceptual views on the activities of the armed forces of the Russia Federation in the information space*, 9 September 2000, available at http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, [visited on 29 April 2018].

- US, NATIONAL RESEARCH COUNCIL, *Technology, policy, law, and ethics regarding US acquisition and use of cyber attack capabilities*, National Academies Press, 2000.

- US, *Patriot Act*, Public Law 107-599, section 1016, 26 October 2001, available at https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, [visited on 2 May 2018].

- US, *The National Security Strategy of the United States,* The White House, September 2002, available at https://www.state.gov/documents/organization/63562.pdf, [visited on 23 February 2018].

- US, DoD, OFFICE OF GENERAL COUNSEL, *Legal distinction between preemption, preventive self-defense and anticipatory self-defense*, report from HAYNES, W. J., 16 October 2002,

available at http://library.rumsfeld.com/doclib/sp/2564/2002-10-16%20from%20William%20Haynes%20re%20Legal%20Distinction%20Between%20Preemption,%20Preventive%20and%20Anticipatory%20Self-Defense.pdf, [visited on 1 March 2018].

- US, The *National Strategy to Secure Cyberspace*, The White House, February 2003, available at https://www.nitrd.gov/cybersecurity/documents/NationalStrategytoSecureCyberspace2003.pdf, [visited on 2 January 2018].

- US, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* The White House, February 2003, available at https://www.dhs.gov/xlibrary/assets/Physical Strategy.pdf, [visited on 22 February 2018].

- UK, GOLDMITH, L., Attorney-General Speech in the House of Lords, HL Debates 21 April 2004, 660 c369-372; in "UK materials on International Law", *BYIL*, 75, 2004, p. 822-823.

- US CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 3121.01B, *Standing Rules of Engagement (SROE)/Standing Rules for the Use of Force (SRUF) for U. S. Forces*, 13 June 2005, available at http://www.loc.gov/rr/frd/Military Law/pdf/OLH 2015 Ch5.pdf, [visited on 22 May 2018].

- F. R. GERMANY, FEDERAL MINISTRY OF DEFENSE, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, 2006, available at http://responsibilitytoprotect.org/Germany White Paper 2006.pdf, [visited on 1 January 2018].

- US, *Information Operations and Cyberwar: Capabilities and Related Policy Issues,* CRS Report for Congress, updated September 2006, available at https://fas.org/irp/crs/RL31787.pdf, [visited on 22 May 2018].

- US, DoD, *The National Military Strategy for Cyberspace Operations*, December 2006, available at file:///C:/Users/hamed/Downloads/35693%20(6).pdf, [visited on 22 March 2018].

- UK GOVERNMENT, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, June 2009, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/file/228841/7642.pdf, [visited on 12 February 2018].

- US NATIONAL RESEARCH COUNCIL, *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*, National Academies Press, 2009.

- US AIR FORCE, *Cyber Operations. Air Force Doctrine Document 3-12*, 15 July 2010, available at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-060.pdf, [visited on 10 March 2018].

- US *Joint Terminology for Cyberspace Operation,* 2010, available at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, [visited on 6 March 2018].

- US, COMMITTEE ON DETERRING CYBERATTACKS, *Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for US policy*, The National Academies Press, 2010.

- AUSTRALIAN GOVERNMENT, *Critical infrastructure resilience strategy*, 2010, available at https://www.tisn.gov.au/Documents/+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf, [visited on 3 March 2018].

- SPAIN, *Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas*, 28 April 2011, *BOE,* 29 April 2011.

- SPAIN, *Real Decreto 704/2011, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*, 20 May 2011, *BOE,* 21 May 2011.

- US, *International strategy for cyberspace. Prosperity, security, and openness in a networked world,* the White House, May 2011, available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, [visited on 11 June 2018].

- US, DoD CYBERSPACE POLICY REPORT, *A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, November 2011, available at https://assets.documentcloud.org/documents/266862/department-of-defense-cyberspace-policy-report.pdf, [visited on 22 February 2018].

- US, DoD, *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories,* November 2011, available at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, [visited on 22 June 2018].

- DUTCH GOVERNMENT, AIV/CAVV, *Cyber Warfare*, Doc. No 77, AIV/No 22, CAVV, December 2011, available at https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf, [visited on 25 February 2018

- US, *Presidential Policy Directive/PPD-20*, of October 2012, available at https://fas.org/irp/offdocs/ppd/ppd-20.pdf, [visited on 22 June 2018].

- GOVERNO ITALIANO, *La posizione italiana sui principi fondementali di internet*, of 17 September 2012, available at http://download.repubblica.it/pdf/2012/tecnologia/internet.pdf,[visited on 25 May 2018].

- PERMANENT MISSION OF FEDERAL REPUBLIC OF GERMANY TO THE UNITED NATIONS, Note No. 516/2012, 5 November 2012.

- SPAIN, *National Cyber Security Strategy,* 2013, available at https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf, [visited on 22 May 2018].

- US, *Executive Order-Improving Critical Infrastructure Cybersecurity*, 12 February, 2013, available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, [visited on 2 April 2018].

- US, *Information operations, Join Publication 3-13,* 27 November 2012, Incorporating Change 1, 20 November 2014, available at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, [visited on 3 March 2018].

- US, DoD, *Cyber Strategy*, 17 April 2015, available at https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, [visited on June 2018].

- US, EGAN, B., Legal Advisor of the US Department of State, speech on the legal aspect of the fight of the US against the Daesh, 1st April 2016, available at https://2009-2017.state.gov/s/l/releases/remarks/255493.htm, [visited on 2 May 2018].

- UK, The Government's policy on the use of drons for targeted killing, Second Report of Session 2015–16, HC 574, HL Paper, 10 May 2016, available at https://publications.parliament.uk/pa/jt201516/jtselect/jtrights/574/574.pdf, [visited on 2 April 2018].

- UK, Cameron *Statement in the House of Commons on His Response to the Foreign Affairs Select Committee (FAC) Report on Military Operations in Syria*, 26 November 2015, available at https://www.gov.uk/government/speeches/pm-statement-responding-to-fac-report-on-military-operations-in-syria, [visited on 23 March 2018].

- US *Strategic Cyberspace Operations Guide*, Army War College, June 2016, available at https://info.publicintelligence.net/USArmy-StrategicCO.pdf, [visited on 14 January 2018].

- UK, *National Cyber Security Strategy 2016-2021*, October 2016, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, [visited on 4 March 2018].

- US, *Report on the legal and policy frameworks guiding the United States' use of military force and related national security operations*, The White House, December 2016, available at https://www.justsecurity.org/wp-content/uploads/2016/12/framework.Report_Final.pdf, [visited on 2 January 2018].

- US, DoD, "Statement from Pentagon Spokesman Capt. Jeff Davis on US strike in Syria", *News Release*, 6 April 2017, available at https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1144598/statement-from-pentagon-spokesman-capt-jeff-davis-on-us-strike-in-syria/, [visited on 23 February 2018].

- UK, FOREIGN AND COMMONWEALTH OFFICE, "Response to General Assembly Resolution 71/28 'Developments in the field of information and telecommunications in the context of international security'", July 2017, available at https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/09/UK-ES-and-full.pdf, [visited on 22 June 2018].

- US, DoD, *Dictionary of Military and Associated Terms*, March 2018, available at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf, [visited on 23 June 2018].

- UK Attorney General Jeremy Wright QC MP, "Cyber and International Law in the 21st century", 23 May 2018, available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, [visited on 23 June 2018].

- F. R. GERMANY GOVERNMENT "German could dispatch armed forces in response to cyberattacks", 6 Jun 2018, available at https://global.handelsblatt.com/politics/germany-soldiers-combat-cyberattacks-931929, [visited on 25 June 2018].

- US, Join Publication 3-12, Cyberspace operations, 8 June 2018, available at https://fas.org/irp/doddir/dod/jp3_12.pdf, [visited on 29 June 2018].

E. **Other documents**

- IDI, *The principle of Non-Intervention in Civil Wars*, 8th Commission, 1975, available at http://www.idi-iil.org/app/uploads/2017/06/1975_wies_03_en.pdf, [visited 20 June 2018].

- "The facts are clear and compelling. The information presented points conclusively to an Al-Qaida role in the 11 September attacks", Statement at NATO Headquarters, 2 October 2001, available at https://www.nato.int/docu/speech/2001/s011002a.htm, [visited on 15 March 2018].

- Written evidence submitted by Daniel Bethlehem QC, Director of Lauterpacht Research Centre for International Law, University of Cambridge, on 7 June 2004, available at https://publications.parliament.uk/pa/cm200304/cmselect/cmfaff/441/4060808.htm, [visited 20 June 2018].

- ICRC, *Rules of International Humanitarian Law and Other Rules Relating to the Conduct of Hostilities*, 20 June 2005.

- The *Chatham House Principles of International Law on the use of force in self-defense*, 2005, published in *ICLQ*, 55(4), 2006, p. 963-972.

- ICC, ASSEMBLY OF STATES PARTIES, *Informal inter-Sessional meeting of the Special Working Group on the Crime of Aggression*, 5th Session, Doc. ICC-ASP/5/SWGCA/INF.1, of 5 September 2006.

- ICC, ASSEMBLY OF STATES PARTIES, *Report of the Special Working Group on the Crime of Aggression*, 5th Session, Doc. ICC-ASP/5/SWGCA/1, 29 November 2006.

- IDI, "Present problems of the use of armed force in International Law. A. Self-defence", Tenth Commission, 27 October 2007, *Annuaire de l'Institut de Droit International,* vol. 72.

- IDI, "Present problems of the use of armed force in International Law. Humanitarian action", Tenth Commission, 27 October 2007, *Annuaire de l'Institut de Droit International*, vol. 72, 2007.

- "Israel's Bombardment of Gaza is not self-defence – It's a War Crime", *Sunday Times*, of 11 January 2009.

- ILA, *Non-State actors in International Law: aims, approach and scope of project and legal issues*, First Report of the Committee: Non-State Actors, The Hague Conference, 2010, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2238750, [visited on 25 May 2018].

- SCHRIJVER, N.; VAN DEN HERIK, L., *Leiden Policy Recommendations on counter-terrorism and International Law* 1 April 2010, published in *NILR,* 57(3), 2010, p. 531-550.

- ICRC, *International humanitarian law and challenges of contemporary armed conflict*, Doc 311C/11/5.1.2, October 2011.

- HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, CUP, 2013.

- INTERNATIONAL GROUP OF EXPERTS, *Tallinn Manual on the International Law applicable to cyber warfare*, CUP, 2013.

- ILA, *Report on aggression and the use of force,* Committee on the Use of Force, Washington Conference, 2014, available at file:///C:/Users/hamed/Downloads/Conference%20Report%20Washington%202014..pdf , [visited on 25 June 2018].

- ILA, *Draft Report on aggression and the use of force,* Committee on the Use of Force, Johannesburg Conference, 2016, available at file:///C:/Users/hamed/Downloads/Draft%20Conference%20Report%20Johannesburg%202016.%20(4).pdf, [visited on 25 June 2018].

- INTERNATIONAL GROUP OF EXPERTS, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, CUP, 2017.

- “Digital policy trend in June”, *Geneva Digital Watch, 22, 30 June 2017,* available at https://dig.watch/DWnewsletter22, [visited on 23 June 2018].

- JAQUEMET, L., “Syria is now international armed conflict”, available at http://www.sbs.com.au/news/article/2017/04/08/syria-now-international-armed-conflict, [visited on 8 April 2017].

-RULAC, “Syria”, available at http://www.rulac.org/browse/countries/syria#collapse1accord, [visited on 20 January 2018].

- “Turkish jets hammer Syrian town to oust US-backed Kurdish militia”, *CNN News*, 21 January 2018, available at https://edition.cnn.com/2018/01/20/middleeast/turkey-syria-military-operation/index.html, [visited on 20 June 2018].

- LUBELL, M.; BARRINGTON, L., “Israel Jet shot down after bombing Iranian site in Syria”, *Reuters*, 10 February 2018, available at https://www.reuters.com/article/us-israel-iran/israeli-jet-shot-down-after-bombing-iranian-site-in-syria-idUSKBN1FU07L, [visited on 20 June 2018].

- “Israel Launches ‘large-Scale’ attack in Syria after fighter jet crashes”, *The Guardian*, 10 February 2018.

- “US supports Israel right to defend itself: pentagon”, *Reuters*, 10 February 2018, available at https://www.reuters.com/article/us-mideast-crisis-syria-israel-usa/u-s-supports-israels-right-to-defend-itself-pentagon-idUSKBN1FU0YV, [visited on 14 July 2018].

- "Statement attributable to the Spokesman for the Secretary-General on the Syrian Arab Republic United Nations Secretary-General", 11 February 2018, available at https://www.un.org/sg/en/content/sg/statement/2018-05-10/statement-attributable-spokesman-secretary-general-situation-middle, [visited on 20 June 2018].

- “Tension rises between Israel and Iran after Syria clash”, *The Wall Street Journal*, 11 February 2018.

- “Lebanon asked UN Security Council to pressure Israel after ‘airspace violation’”, A*rab News,* 11 February 2018.

- “Hezbollah: downing of Israeli F-16 marks ‘start of new strategic phrase’”, *Haaretz,* 11 February 2018.

- “EU warns of spiralling violence after Israel–Syria border incident”, *Reuters*, 12 February 2018 available at https://www.google.com/search?ei=15sqW9raNOqZgAbktamQBA&q=EU+warns+of+spiralling+violence+after+Israel%E2%80%93Syria+border+incident&oq=EU+warns+of+spiralling+violence+after+Israel%E2%80%93Syria+border+incident&gs_l=psy-

ab.12...0.0.0.4771.0.0.0.0.0.0.0.0..0.0....0...1c..64.psy-ab..0.0.0....0.H47-DkWmlWQ, [visited on 20 June 2018].

DOCTRINE

A. *The prohibition of the use of force and the right of self-defence*

- AHMED, D., "Defending weak States against the unwilling or unable doctrine of self-defence", *Journal of International Law and International Relations*, 9, 2013, p. 1-37.

- AKANDE, D.; LIEFLÄNDER, Th., "Self-defence against non-State actors (continuation of the debate). Clarifying necessity, imminence, and proportionality in the law of self-defense", *AJIL*, 107(3), 2013, p. 563-570.

- ALDER, M. C., *The inherent right of self-defence in International Law,* Springer, 2013.

- ALOYO, E., *The last of last resort*, The Hague Institute for Global Justice, Working Paper 1, July 2014.

- ALCAIDE, J., "La guerra contra el terrorismo: ¿una OPA hostil al Derecho de la comunidad internacional?", *REDI*, 53(1/2), 2001, p. 289-302.

- ALEXANDROV, S. A., *Self-defense against the use of force in international law*, Kluwer, 1996.

- ALLO, A. K., "Ethiopia's armed intervention in Somalia: the legality of self-defence in response to the threat of terrorism", *Denver Journal of International Law & Policy,* 39, 2010, p. 139-167.

- ALMUKHTAR, S., *et al*., "Mapping the targets of the American military attack on Syria", *The New York Times*, available at https://www.nytimes.com/interactive/2017/04/07/world/middleeast/us-syria-missile-attack-airbase.html,]visited on 21 June 2018[.

- ANDRÉS, P., "Las normas relativas al uso de la fuerza: la seguridad colectiva y la legitima defensa en el context de la reforma de las Naciones Unidas", in GARCIA, C; RODRIGO, A. J. (eds.), *La seguridad comprometida: nuevos desafios, amenazas y conflictos armadas*, Tecnos, 2008, p. 113-125.

- ANTONOPOULOS, C., "Force by armed groups as armed attack and the broadening of self-defence", *NILR,* 55(2), 2008, p. 159-180.

- ARAI-TAKAHASHI, Y., "Shifting boundaries of the right sellf-defence. Appraising the impact of the September 11 attacks on *Jus ad bellum*", *The International Lawyer*, 36(4), 2002, p. 1081-1102.

- AREND, A. C., "International law and the pre-emptive use of military force", *The Washington Quarterly,* 26(2), 2003, p. 89-103.

- AREND, A. C.; BECK, R. J., *International Law and the use of force: beyond the UN Charter paradigm*, Routledge, 2013.

- ARIAS, G. J., "Are the rules for the right to self-defence outdated to address current conflicts like attacks from non-State actors and cyber attacks?", *Revista Tribuna Internacional*, 6(11), 2017, p. 1-19.

- ARMSTRONG, A.; REISMAN, M., "The past and future of the claim of preemptive self-defense", *AJIL*, 100(3), 2006, p. 525-550.

- ASRAT, B., *Prohibition of force under the UN charter: a study of art. 2 (4)*, Iustus, 1991.

- AUST, A., *Modern treaty law and practice*, CUP, 2013.

- AZAROVA, V.; BLUM, I., "Belligerency", in LACHENMANN, F.; WOLFRUM, R. (eds.), *The law of armed conflict and the use of force: the Max Planck Encyclopedia of Public International Law*, 2, OUP, 2017, p. 111-116.

- AZUBUIKE, E. Ch., "Proving the scope of self-defence in International Law", *Annual Survey of International and Comparative Law*, 17(1), 2011, p. 129-183.

- BAETENS, F., "Hague Conferences (1899, 1907)", *Oxford Bibliographies online*, 2012, available at http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0115.xml, [visited on 24 June 2018].

- BAKIRCIOGLU, O., "The right to self-defence in national and International Law: the role of the imminence requirement", *Indiana International and Comparative Law Review*, 19(1), 2009, p. 1-48.

- BANNELIER, K., "Military interventions against ISIL in Iraq, Syria and Libya and the legal basis of consent, *Leiden Journal of International Law*, 29(3), 2016, p. 743-775.

- BASSIOUNI, M. CH., "The new wars and the crisis of compliance with the law of armed conflict by non-state actors", *The Journal of Criminal Law and Criminology,* 98(3), 2008, p. 711-810.

- BECKER, J. D. "The continuing relevance of article 2 (4): a consideration of the status of the UN Charter's limitations of the use of force", *Denver Journal of International Law and Policy,* 32(3), 2004, p. 583-609.

- BEKKER, P. H. F., "oil Platforms (Iran *v.* United States)", *AJIL*, 98(3), 2004, p. 550-558.

- BELLAL, A, (ed.), *The War Report: armed conflict in 2014*, OUP, 2015.

- BELLIER, S., "Unilateral and multilateral preventives self-defense", *Maine Law Review*, 58 (2), 2006, p. 508-542.

- BENNETT, T. W., "A linguistic perspective of the definition of the aggression", *GYIL*, 31, 1988, p. 48-69.

- BERDUD, CARLOS ESPALIÚ, "The EU response to the Paris terrorist attacks and the reshaping of the rights to self-defence in International Law", *Spanish Yearbook of International Law,* 20, 2016, p. 183-207.

- BERES, L. R., "Israel, Iran and pre-emption: choosing the least unattractive option under International Law", *Dickinson Journal of International Law,* 14(2), 1996, p. 187-206.

- BERMEJO, R., *El marco jurídico internacional en material de uso de la fuerza: ambigüedades y limites,* Civitas, 1993.

- BERMEJO, R., "El Derecho Internacional frente al terrorismo: ¿nuevas perspectivas tras los atentados del 11 de septiembre?", *AEDI*, 17, 2001, p. 5-24.

- BERMEJO, R., "La legítima defensa y el Derecho Internacional en los albores del siglo XXI", in *Los nuevos escenarios internacionales y europeos del derecho y seguridad*, Colección Escuela Diplomática, 7, 2003, p. 127-141.

- BERMEJO, R., "El uso de la fuerza, la Sociedad de las Naciones Unidas y el Pacto Briand-Kellog", in GAMARRA, Y.; FERNANDEZ, C. (coords.), *Los orígenes del Derecho Internacional contemporaneo. Estudios conmemorativos del centenario de la Primera Guerra Mundial,* Institucion Fernando el Catolico, 2015, p. 217-245.

- BETHLEHEM, D., "Self-defense against an imminent or actual armed attack by non-State actors", *AJIL*, 106(4), 2012, p. 769-777.

- BETHLEHEM, D., "Principles of self-defence. A brief response", *AJIL*, 107(3), 2013, p. 579-585.

- BLIX, H., "Legal restraints on the use of armed force", in ENGDAHL, O.; WRANGE, P., *Law at war: the law as it was and the law as it should be*, Martinus Nijhoff, 2008, p. 21-38.

- BLOKKER, N. M.; SCHRIJVER, N. (eds.), *The security Council and the use of force: theory and reality-a need for change?*, Martinus Nijhoff, 2005.

- BODANSKY, D.; GATHII, J. T., "ICJ-prohibition against the use of force-self-defence under article 51 of the UN Charter-duty of vigilance-IHR and IHL under belligerent occupation", AJIL, 101(1), 2007, p. 142- 149.

- BOER, L. J., "'Echoes of time past' on the paradoxical nature of article 2(4)", *JCSL*, 20(1), 2014, p. 5-26.

- BONAFEDE, M. C., "Here, there, and everywhere: assessing the proportionality doctrine and US uses of force in response to terrorism after the September 11 attacks", *Cornell Law Review,* 88, 2002, p. 155- 214.

- BOTHE, M., "Terrorism and the legality of pre-emptive force", *EJIL*, 14(2), 2003, p. 227-240.

- BOTHE, M., "The protection of the civilian population and NATO bombing on Yugoslavia: comments on a report to the prosecutor of the ICTY", *EJIL,* 12(3), 2001, p. 531-536.

- BOWETT, D. W., "Collective self-defence under the Charter of the United Nations", *BYIL*, 32, 1955-1956, p. 130-161.

- BOWETT, D. W., *Self-defence in International Law*, Praeger, 1958.

- BOWETT, D. W., "Reprisal involving recourse to armed force", *AJIL,* 66, 1972, p. 1-36.

- BOYLE, F., "The Entebbe hostage crisis", *NILR*, 29(1), 1982, p. 32-71.

- BRENNER, Ph., "Cuba and the Missile Crisis", *Journal of Latin American Studies.* 22(1), 1990, p. 115-142.

- BRING, O., "The use of force under the UN Charter: modification and reform through practice or consensus", in EBBESSON, J., *et al*. (eds.), *International law and changing perceptions of security: liber amicorum Said Mahmoudi*, Martinus Nijhoff, 2014, p. 1-13.

- BROWN, A. C., "Hard cases make bad laws: an analysis of State-sponsored terrorism and its regulation under International Law", *Journal Armed Conflict Law,* 2, 1997, p. 135-176.

- BROWNLIE, I., *International Law and the use of force by States*, Clarendon Press, 1963.

- BRUNNÉE, J.; TOOPE, S. J., "The use of force: International Law after Iraq", *ICLQ*, 53(4), 2004, p. 785-806.

- BRUNNÉE, J., "The security Council and self-defence: which way to global security?", in BLOKKER, N.;M.; SCHRIJVER, N.(eds.), *The Security Council and the use of force: theory- a need for change?*, Martinus Nijhoff, 2005, p. 107-132.

- BRUNNÉE, J.; TOOPE, S. J., "Self-defence against non-State actors: are powerful States willing but unable to change International Law", *ICLQ*, 67(2), 2018, p. 263-286.

- BYERS, M., "Terrorism, the use of force and International Law after 11 September", *ICLQ,* 51(2), 2002, p. 401-414.

- BYERS, M., "Pre-emptive self-defence: hegemony, equality and strategies of legal change", *Journal of Political Philosophy*, 11 (2), 2003, p. 171-190.

- BYERS, M., "The intervention in Afghanistan-2001", in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 626-638.

- BYRNES, A., *et al.* (eds.), *International Law in the new age of globalization,* Martinus Nijhoff, 2013.

- CARTER, B. E.; WEINER, A. S., *International Law*, sixth edition, Wolters Kluwer Law & Business, 2011.

- CANNIZZARO, E., "The role of proportionality in the law of international countermeasures", *EJIL*, 12 (5), 2001, p. 889-916.

- CANNIZZARO, E.; PALCHETTI, P. (eds.), *Customary International Law on the use of force. A methodological approach*, Martinus Nijhoff, 2005.

- CANNIZZARO, E., "Contextualizing proportionality: *ius ad bellum* and *ius in bello* in the Lebanese war", *International Review of the Red Cross*, 88, 2006, p. 779-792.

- CANNIZZARO, E.; RASI, A., "The US strikes in Sudan and Afghanistan-1998", in RUYS, T.; *et al*. (eds.), *The use of force in International Law. A case-based approach*, OUP, 2018, p. 541-551.

- CANOR, I., "When *jus ad bellum* meet *jus in bello*: the occupier's right of self-defence against terrorism stemming from occupied terrories", *Leiden Journal of International Law*, 19(1), 2006, p. 129-149.

- CASANOVAS, O., "El principio de prohibición del uso de la fuerza", in DIEZ DE VELASCO, *Instituciones de derecho internacional público*, 18ª ed., Tecnos, 2013, p. 1067-1096.

- CASANOVAS, O.; RODRIGO, A., *Compendio de Derecho Internacional público*, 7ª ed., Tecnos, 2018.

- CASSESE, A., *International Law,* OUP, 2005.

- CASSESE, A., "Article 51", in COT, J. P.; *et al*. (eds.), *La Charter des Nations Unies, commentaire article par article*, Economica, 3rd ed., 2005, p. 1329-1360.

- CASTREN, E., *Civil war*, Suomalainen Tiedeakatemia, 1966.

- CENIC, S., "State responsibility and self-defence in International Law post 9/11: has the scope of article 51 of the United Nations Charter been widened as a result of the US response to 9/11?", *Australian International Law Journal*, 14, 2007, p. 201-216.

- CERVELL, M. J., *La legítima defensa en Derecho Internacional contemporáneo*(*Nuevos tiempos, nuevos actors, nuevos retos*), Tirant lo Blanch, 2017.

- CERVELL, M. J., "Sobre la doctrina <unwilling or unable State> (i podria el fin justificar los medios?)", *REDI*, 70(1), 2018, p. 77-100.

- CORN, G. S., *et al.* (eds.), *US military operations: law, policy, and practice*, OUP, 2016.

- KU, CH.; JACOBSON, H. K. (eds.), *Democratic accountability and the use of force in International Law*, CUP, 2002.

- CHAINOGLOU, K., "Reconceptualising self-defence in International Law", *King's Law Journal*, 18(1), 2007, p. 61-94.

- CHAINOGLOU, K., *Reconceptualising the law of self-defence*, Bruylant, 2008.

- CHAN, K., "State failure and the changing face of the *jus ad bellum*", *JCSL,* 18(3), 2013, p. 395-426.

- CHARNEY, J. I., "Anticipatory humanitarian intervention in Kosovo", *AJIL,* 93(4), 1999, p. 834-841.

- CHARNEY, J. I., "The use of force against terrorism and International Law", *AJIL*, 95(4), 2001, p. 835-839.

- CHENEVIER, J., "Oil on troubled waters—The ICJ tackles use of force", *The Cambridge Law Journal,* 63(1), 2004, p. 1-4.

- CHENG, B., "Pre-emptive or similar type of self-defence in the territory of foreign States", *Chinese Journal of International Law*, 12, 2013, p. 1-8.

- CHRISTODOULIDOU, T.; CHAINOGLOU, K., "'The principle of proportionality in self-defence and humanitarian intervention", *Journal of International Law of Peace and Armed Conflict*, 20, 2007, p. 79-90.

- COHEN, A, (eds.), *Rethinking the law of armed conflict in an age of terrorism*, Lexington Books, 2012.

- COLL, A., "The legal and moral adequacy of military responses to terrorism", *American Society of International Law Proceedings*, 81, 1987, p. 297-307.

- CONDORELLI, L., "The imputability to States of acts of international terrorism", *Israel Yearbook on Human Rights*, 1989, p. 233-246.

- CONDORELLI, L., "Les attentats du 11 Septembre et leurs suites: Où va le droit international?", *RGDIP*, 105 (4), 2001, p. 829-848.

- CONTE, A., "The war on terror: self-defence or aggression?", in DOLGOPOL, U.; GARDAM, J. G.(eds.), *The challenges of conflict: International Law respond*, Martinus Nijhoff, 2006, p. 393-411.

- CORTEN, O.; DUBUISSON, F., "Opération "liberté immuable": une extension abusive du concept de légitime défense", *RGDIP*, 106(1), 2002, p. 51-77.

- CORTEN, O., "The controversies over the customary prohibition on the use of force: a methodological debate", *EJIL*, 16 (5), 2005, p. 803-822.

- CORTEN, *O., The law against war: the prohibition on use of force in contemporary International Law,* Hart, 2010.

- CORTEN, O., "Regulating resort to force: a response to Mathew Waxman from a 'Bright Liner'", *EJIL*, 24, 2013, p. 191-197.

- CORTEN, O., "La rébellion et le Droit International: le principe de neutralité en tension", *RCADI*, 374, 2014, p. 53-312.

- CORTEN, O., "The 'unwilling or unable' test: has it been, and could it be, accepted?", *LJIL,* 29, 2016, p. 777-799.

- CORTEN, O., "The military operations against the 'Islamic State' (ISIL or Daesh)-2014" in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 873-898.

- COUZIGOU, I. "The fight against the 'Islamic State' in Syria: towards the modification of the right to self-defence?", *Geopolitics, History, and International Relations,* 9(2), 2017, p. 80-106.

- CROOK, J. R., "US efforts to enhance cybersecurity and to counter international theft of trade secrets", *AJIL*, 107(2), 2013, p. 447-449.

- CULLEN, A., *The concept of non-international armed conflict in International Humanitarian Law*, 66, CUP, 2010.

- D'AMATO, A., "Israel's air strike upon the Iraqi nuclear reactor", *AJIL,* 77(3), 1983, p. 584-588.

- DE SOUZA, I. M. L., "Revisiting the right of self-defence against non-State armed entities", *CYIL*, 53, 2015, p. 202-243.

- DEEKS, A., "Unwilling or unable: toward a normative framework for extra-territorial self-defence", *Virginia Journal of International Law*, 52(3), 2012, p. 483-551.

- DEEKS, A. S., "Taming the doctrine of pre-emption", in WELLER, M.; *et al.* (eds.), *The Oxford handbook of the use of force in International Law,* OUP, 2015, p. 661-678.

- DELBRUCK, J., "The fight against global terrorism: self-defence or collective security as international policy action? Some comments on the international legal implications of the war on terrorism", *GYIL*, 44, 2002, p. 9-24.

- DEL VALLE, A., "Legítima defensa ? Primer balance para el Derecho Internacional tras los atendados del 11 de septiembre de 2001", *Tiempo de Paz*, 64, 2002, p. 6-17.

- DELANIS, J. A., "Force under article 2(4) of the United Nations Charter: the question of economic and political coercion", *VJTL*, 12, 1979, p. 101-130.

- DE MARCO, G.; BARTOLO, M., *A second generation United Nations: for peace and freedom in the 21st Century*, Routledge, 2009.

- DEMPSEY, P. S., "Economic aggression & (and) self-defence in International Law: the arab oil weapon and alternative American responses thereto", *Case Western Reserve Journal of International Law*, 9(2), 1977, 253-321.

- DHOKALIA, R. P., "Civil Wars and International Law", *Indian Journal of International Law,* 11, 1971, p. 219-224.

- DINSTEIN, Y., *The International Law of belligerent occupation*, CUP, 2009.

- DINSTEIN, Y., *War, aggression and self-defense*, 6th ed., CUP, 2017.

- DUPUY, R.J., "Droit d'ingerence et assistance humanitaire", in Homage to professor M. DIEZ de VELASCO, *Hacia un nuevo orden internacional y Europeo*, Tecnos, 1993, p. 273-280.

- EBBEN, I., "The use of force against a non-State actor in the territory of another State: applying the self-defence framework to Al-Qaeda", 2011, p. 1-51, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960508, [visited on 21 June 2018].

- ECKERT, A. E.; MOFIDI, M., "Doctrine or doctrinaire-the first strike doctrine and preemptive self-defence under International Law, *Tulane Journal of International and Comparative Law*, 12, 2004, p. 117-151.

- EGEDE, E.; STUTCH, P., *Politics of International Law and international justice*, Edinburgh University Press, 2013.

- EICHENSEHR, K. E., "Targeting Tehran: assessing the lawfulness of pre-emptive strikes against nuclear facilities", *UCLA Journal of International Law and Foreign Affairs*, 11, 2006, p. 59-93.

- ENABULELE, A. O., "Use of force by international/regional non-State actors: no armed attack, no self-defence", *European Journal of Law Reform*, 12, 2010, p. 209-229.

- ERICKSON, R. J., *Legitimate use of military force against State-sponsored international terrorism*, Air University Press, 1989.

- ETEZAZIAN, S., "The nature of the self-defence proportionality requirement", *JUFIL*, 4(2), 2017, p. 260-289.

- FALK, R. A., "Janus tormented: the International Law of internal war", in ROSENAU, J. N. (ed.), *International aspects of civil strife*, Princeton Legacy Library, 1964, p. 185-248.

- FARER, T. J., "Political and economic aggression in contemporary International Law", in CASSESE, A. (ed.), *The current regulation of the use of force,* Martinus Nijhoff, 1986, p. 121-132.

- FARHANG, C., "Self-defense as circumstance precluding the wrongfulness of the use of force", Utrecht Law Review, 11, 2015, p. 1-18.

- FEINSTEIN, B. A., "Operation enduring freedom: legal dimensions of an infinitely just operation", Journal of Transnational Law & Policy, 11, 2001, p. 201-258.

- FINKELSTEIN, C. D., "Self-defense as a rational excuse", University of Pittsburgh Law Review., 57, 1995, p. 621- 647.

- FISCHER, G., "Le bombardement par Israël d'un réacteur nucléaire irakien", *AFDI*, 27, 1981, p. 147-167.

- FISK, K.; RAMOS, J. M., "Actions speak louder than words: preventive self-defence as a cascading norm", *International Studies Perspectives*, 15(2), (2014). p. 163-185.

- FISK, K.; RAMOS, J. M. (eds.), *Preventive force: drones, targeted killing, and the transformation of contemporary warfare*, New York University Press, 2016.

- FITZMAURICE, G. G., "The definition of aggression", *ICLQ*, 1(1), 1952, p. 137-144.

- FLACH, O., "The exercise of self-defence against ISIL in Syria: new insights on the extraterritorial use of force against non-State actors", *JUFIL*, 3(1), 2016, p. 37-69.

- FLORY, M., "L'Organisation des Nations Unies et les opérations de maintien de la paix", *AFDI*, 11, 1965, p. 446-468.

- FOCARELLI, C., "The responsibility to protect doctrine and humanitarian intervention: too many ambiguities for a working doctrine", *JCSL*, *13*(2), 2008, p. 191-213.

- FOLEY, B. J., "Avoiding a death dance: adding steps to the International Law on the use of force to improve the search for alternatives to force and prevent likely harms", *Brooklyn Journal of International Law*, 29(1), 2003, p. 129-173.

- FRANCHINI, D.; TZANAKOPOULOS, A., "The Kosovo crisis-1999", in RUYS, T., *et al*. (eds.), *The use of force in International Law. A case-based approach*, OUP, 2018, p. 594-622.

- FRANCIONI, F., "Balancing the prohibition of force with the need to protect human right: a methodological approach", in CANNIZZARO, E.; PALCHETTI, P. (ed.), *Customary international law on the use of force. A methodological approach*, Martinus Nijhoff, 2005, p. 269-292.

- FRANCK, Th. M., "Who killed article 2(4)? or: changing norms governing the use of force by States", *AJIL*, 64(5), 1970, p. 809-837.

- FRANCK, Th. M., "Terrorism and the right of self-defence", *AJIL,* 95(4), 2001, p. 839-843.

- FRANCK, Th. M., *Recourse to force: State action against threats and armed attacks*, CUP, 2002.

- FRANCK, Th. M., "In extremis: are there principles applicable to the illegal use of force?", in CASSESSE, A.; VOHRAH, L. C. (eds.)., *Man's inhumanity to man: essays on International Law in honour of Antonio Cassese*, 5, Martinus Nijhoff, 2003, p. 309-351.

- GARCÍA, E. M., "La legítima defensa en el Derecho Internaconal contemporáneo: ¿algo nuevo bajo el sol tras la sentencia de la CIJ sobre el asunto de las plataformas petrolíferas", *REDI*, 55(2), 2003, p. 819-838.

- GARDAM, J., "Proportionality and force in International Law", *AJIL,* 87(3), 1993, p. 391-413.

- GARDAM, J., *Necessity, proportionality and the use of force by States*, 35, CUP, 2004.

- GARDAM, J., "A role for proportionality in the war on terror", *NJIL*, 74(3), 2005, p. 3-25.

- GARWOOD-GOWERS, A., "Pre-emptive self-defence: a necessary development or the road to international anarchy, *Australian Yearbook of International Law,* 23, 2004, p. 51-72.

- GASSER, H.P., "Notes on the law on belligerent occupation", *Revue de Droit Militaire et de Droit de la Guerre*, 45, 2006, p. 229-238.

- GATHII, J. T., "Irregular force and self-defence under the UN Charter", in O'CONNELL, M. E. (ed.), *What is war? An investigation in the wake of 9/11*, Brill, 2012, p. 97-108.

- GRAHAM, Th, "National self-defence, International Law, and weapons of mass destruction", *Chicago Journal of International Law,* 4, 2003, p. 1-17.

- GAZZINI, T., *The changing rules on the use of force in International Law*, Manchester University Press, 2005.

- GAZZINI, T., "The rules on the use of force at beginning of the XXIX Century", *Journal of Conflict and Security Law*, 11(3), 2006, p. 319-342.

- GAZZINI, T.; TSAGOURIAS, N. (eds.), *The use of force in International Law*, Routledge, 2016.

- HAMID, A. G., "The legality of anticipatory self-defence in the 21st Century world order: a re-appraisal", *NILR,* 54(3), 2007, p. 441-490.

- GILL, T. D., "The temporal dimension of self-defense: anticipation, pre-emption, prevention and immediacy", in SCHMITT, M.; PEJIC, J. (eds.), *International Law and armed conflict: exploring the faultlines*, Brill, 2007, p. 113-156.

- GILL, T. D.; FLECK, D. (eds.), *The handbook of the International Law of military operations,* 2nd ed., OUP, 2015.

- GLASSMAN, A., "Evolution of the prohibition on the use of force and its conflict with human rights protection: balancing equally forceful *jus cogens* norms", *UCLA Journal International Law and Foreign Affairs,* 16, 2011, p. 345-384.

- GLENNON, M. J., "The fog of law: self-defence, inherence, and incoherence in article 51 of the United Nations Charter", *Harvard Journal on Law and Public Policy,* 25, 2002, p. 539-558.

- GLENNON, M. J., "The rise and fall of the UN Charter's use of force rules", *Hastings International and Comparative Law Review,* 27, 2003, p. 497-510.

- GLENNON, M. J., "The emerging use of force paragim", *Journal of Conflict and Security Law*, 11(3), 2006, p. 309-317.

- GOGGIN, S., "Self-defence, the Security Council and judicial review", *Sri Lanka Journal of International Law*, 17, 2005, p. 138-166.

- GONZALEZ, J. A., "Los atentados del 11 de septiembre, la operación <libertad duradera> y el derecho de legítima defensa", *REDI*, 53(1-2), 2001, p. 247-271.

- GOODRICH, L. M.; *et al*., *Commentaire de la Charte des Nations Unies [signée le 26 juin 1945 à San-Francisco]*, La Baconnière, 1948.

- GOODRICH, L. Y.; *et al*., *Charter of United Nations, Commentary and Documents*, 3rd ed., Columbia University Press, 1969.

- GORDON, E., "Article 2 (4) in historical context", *YJIL,* 10(4), 1984, p. 271-278.

- GRAHL-MADSEM, A., "Decolonization: the modern version of a 'just war'", *BYIL,* 22, 1979, p. 255-273.

- GRAY, C., "The use and abuse of the International Court of Justice: cases concerning the use of force after Nicaragua", *EJIL*, 14(5) 2003, p. 867-905.

- GRAY, C., "The Eritrea/Ethiopia Claims Commission oversteps its boundaries: a partial award?", *EJIL,* 17(4), 2006, p. 699-772.

- GRAY, C., "The International Court of Justice and the use of force", in TAMS, C. J.; SLOAN, J., *The development of International Law by the International Court of Justice*, OUP, 2013, p. 237-262.

- GRAY, C., *International Law and the use of force*, 4th ed., OUP, 2018.

- GRAY, C., "The limits of force", *RCADI*, 376, 2014, p. 93-198.

- GREEN, J. A., “Self-defence: a State of mind for States?”, *NILR*, 55(2), 2008, p. 181-206.

- GREEN, C., *The International Court of Justice and self-defence in International Law*, Hart, 2009.

- GREEN, J. A., "Fluctuating evidentiary standards for self-defence in the International Court of Justice", *ICLQ*, 58(1), 2009, p.163-179.

- GREEN, J. A., "Questioning the peremptory Status of the prohibition of the use of force", *MIJIL,* 32(2), 2011, p. 215-257.

- GREEN, J. A.; GRIMAL, F., "The threat of force as an action in self-defence under International Law", *VJTL,* 44(2), 2011, p. 285-328.

- GREEN, J. A., “The article 51 reporting requirement for self-defence actions”, *Virginia Journal of International Law*, 55(3), 2015, p. 563-625.

- GREENSPAN, M., *The modern law of land warfare,* UCP*,* 1959.

- GREENWOOD, Ch., “The relationship between *jus ad bellum* and *jus in bello*”, *Review of International Studies,* 9(4), 1983, p. 221-234.

- GREENWOOD, Ch., “International Law and the US air operation against Libya”, *West Virginia Law Review, 89,* 1987, p. 953-956.

- GREENWOOD, Ch., “Self-defence and the conduct of international armed conflict”, in DINSTEIN Y.; TABORY, M., (eds.), *International Law at a time of perplexity. Essays in honour of Shabtai Rosenne*, Martinus Nijhoff, 1989, p. 273-288.

- GREENWOOD, Ch., "International Law and the pre-emptive use of force: Afghanistan, Al-Qaida and Iraq", *San Diego International Law Journal,* 4, 2003, p. 7-37.

- GREENWOOD, Ch., “Self-defence”, in *Max Planck Encyclopedia of Public International Law*, 2011, available at http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401?prd=EPIL,]visited on 22 June 2018[.

- GREIG, D. W., “Self-defence and the Security Council: what does article 51 require?, *ICLQ*, 40(2), 1991, p. 366-402.

- GRIMAL, F., *Threats of force: International Law and strategy*, Routledge, 2013.

- GUIORA, A. N., "Anticipatory self-defence and International Law. A re-evaluation", *JCSL*, 13(1), 2008, p. 3-24.

- GUPTA, R., "Recognition of insurgent and belligerent organisations in International Law", 2014, available at https://ssrn.com/abstract=2457749, [visited on 4 June 2018].

- GURULI, E. L. "The terrorism era: should the international community redefine its legal standards on use of force in self-defense?", *Willamette Journal of International Law and Dispute Resolution,* 12(1), 2004, p. 100-123.

- GUTIÉRREZ, C., *El estado de necesidad y el uso de la fuerza en Derecho Internacional*, Tecnos, 1987.

- GUTIÉRREZ, C., *El uso de la fuerza y el Derecho Internacional después de la descolonización,* Universidad de Valladolid, 1988.

- GUTIÉRREZ, C., "¿No cesaréis de citarnos leyes viendo que ceñimos espadas?", *AEDI,* 2001, p. 25-38.

- GUTIÉRREZ, C., *El hecho ilícito internacional*, Dykinson, 2005.

- GUTIÉRREZ, C., "El 'uso de la fuerza' en los Informes del Grupo de Alto Nivel (2004), del Secretario General (2005) y, a la postre, en el Documento Final de la Cumbre de Jefes de Estado y de Gobierno (Naciones Unidas, Nueva York, septiembre de 2005)", *UNISCI Discussion Papers*, 10, 2006, p. 75-100.

- GUTIÉRREZ, C.; CERVELL, M. J., "La prohibición del uso de la fuerza en la sentencia de la CIJ de 19 de diciembre de 2005 (asunto sobre las actividades armadas en el territorio del Congo, Republica Democrática del Congo c. Uganda)", *REDI*, 58(1), 2006, p. 239-256.

- GUTIÉRREZ, C., "La evolución de la prohibición del uso de la fuerza en las relaciones internacionales: políticos *versus* jueces", *Anuario Argentino de Derecho Internacional,* 16(1), 2007, p. 79-98.

- GUTIÉRREZ, C., "Sobre la prohibición del uso de la fuerza armada en los últimos setenta años (1945-2015)", in PONS, X., *Las Naciones Unidas desde España, 70 Aniversario de las Naciones Unidas, 60 Aniversario del ingreso de España en las Naciones Unidas,* ANUE, 2015, p. 125-150.

- HAAS, M. C.; FISCHER. S. Ch., "The evolution of targeted killing practices: autonomous weapons, future conflict, and the international order", *Contemporary Security Policy,* 38(2), 2017, p. 281-306.

- HAKIMI, M., "Defensive force against non-State actors: the state of play", *International Law Studies,* 91, 2015, p. 1-31

- HALBERSTAM, M., "The right to self-defence once the Security Council takes action", *MJIL*, 17(2), 1996, p. 229-248.

- HEHIR, A.; *et al*., "Principle of pre-emption: a commentary on issues and scenarios for self-defence in the 21st Century", in HEHIR, A.; *et al*. (eds.), *International Law, Security and Ethics: Policy Challenges in the Post-9/11 World*, Routledge, 2011.

- HENDERSON, Ch.; GREEN, J. A., "The *ius ad bellum* and entities short of statehood in the Report on the conflict in Georgia", *ICLQ,* 59(1), 2010, p. 129-139.

- HENDERSON, Ch., "Israel military operations against GAZA: operation Cast Lead (2008-2009), operation Pillar of Defence (2012), and Operation protective Edge (2014)", in RUYS, T., *et al*. (eds.), *The use of force in International Law. A case-based approach*, OUP, 2018, p. 729-748.

- HENKIN, L., "The reports of the death of article 2(4) are greatly exaggerated", *AJIL*, 65(3), 1971, p. 544-548.

- HENKIN, L., *How nations behave: law and foreign policy*, CUP, 1979.

- HENKIN, L., *International Law: politics and values*, Dordrecht, 1995.

- HENRIKSEN, A., "*Jus ad bellum* and American targeted use of force to flight terrorism around the world", *JCSL*, 2014, p. 1-40.

- HESELHAUS, S., "International Law and the use of force", in SCHWABACH, A., COCKFIELD, A. J. (eds.), *International Law and institutions*, Encyclopedia of Life Support Systems, 2009, p. 60-87.

- HIGGINS, N., *Regulating the use of force in wars of national liberation: the need for a new regime: a study of the South Moluccas and Aceh*, Brill, 2010.

- HIGGINS, R., *The development of International Law through the political organs of the United Nations*, OUP, 1963.

- HIGGINS, R., "International Law and civil conflict", in LUARD, E. (ed.), *The international regulation of civil wars*, Thames and Hudson, 1972, p. 160-186.

- HIGGINS, R., "The United Nations at 70 years: the impact upon International Law", *ICLQ*, 65(1), 2016, p. 1-19.

- HMOUD, M., "The use of force against Iraq: occupation and Security Council Resolution 1483", *Cornell International Law Journal*, 36(3), p. 435-453.

- HSIAO, ANNE HSIU-AN., "Is China's policy to use force against Taiwan a violation of the principle of non-use of force under International Law?", *New England Law Review,* 32, 1998, p. 715-732.

- MOORE, J. N.; *et al*., "The Bush Administration preemption doctrine and the future of world order: remark", in *Proceeding of* American Society of International Law, 98th Meeting, 2004, p. 325-337.

- HOWARD, M., "*Temperamenta belli:* can war be controlled?", in HOWARD, M. (ed.), *Restraints on war: studies in the limitation of armed conflict*, OUP, 1979, p. 23-35.

- IGLESIAS, J. L., "La prohibición general del recurso a la fuerza i las resoluciones descolonizadoras de la Asamblea General de las Naciones Unidas", *REDI*, 24, 1971, p.173-201.

- IOVANE, M., DE VITTOR, F., "La doctrine européenne et l'intervention en Iraq", *AFDI,* 49, 2003, p. 17-31.

- JAMNEJAD, M.; WOOD, M. "The principle of non-intervention", *LJIL*, *22*(2), 2009, p. 345-381.

- JONES, T., "Who killed the right to self-defence?", in HEHIR, N.; *et al*. (eds.), *International Law, security and ethics: policy challenges in the post-9/11 world*, Routledge, 2011, p. 129-146.

- JOYNER, D. H., "The Kosovo intervention: legal analysis and a more persuasive paradigm", *EJIL,* 13(3), 2002, p. 597-619.

- JIMÉNEZ DE ARECHAGA, E., "International Law in the past third of a Century", *RCADI*, I, 1978, p. 9-343.

- JIMÉNEZ DE ARECHAGA, E., *Derecho Internacional contemporáneo*, Tecnos, 1980.

- KAMMERHOFER, J., "Uncertainties of the law on self-defence in the United Nations Charter", *NYIL,* 35, 2004, p. 143-204.

- KAMTO, M., *L'agression en Droit International",* Pedone, 2010.

- KAYE, D., "Adjudicating self-defence: discretion, perception, and the resort to force in International Law", *Columbia Journal of Transnational Law*, 44(1), 2005, p. 134-184.

- KEOHANE, R. O., "The concept of accountability in world politics and the use of force, *MJIL,* 24(4), 2003, p. 1121-1141.

- KIRCHHOFF, L., *Constructive interventions: paradigms, process and practice of international mediation*, 3, Kluwer Law International, 2008.

- KITTRICH, J., *The right of individual self-defense in Public International Law*, Logos Verlag, 2008.

- KOH, H. H., "The Obama administration and International Law: keynote addressed at the American Society of International Law, 104th Annual Meeting", available at http:// www.state.gov/s/l/releases/remarks/139119.htm, [visited on 8 December 2016].

- KOLB, R.; HYDE, R., An *introduction to the International Law of armed conflicts*, Bloomsbury Publishing, 2008.

- KOLB, R., *International Law on the maintenance of peace*. *Just contra bellum,* Edward Elgar, 2018.

- KOOIJMANS, P. H., "The legality of the use of force in the recent case law of the International Court of Justice", in YEE, S.; MORIN, J. (eds.), *Multiculturalism and International Law: essay in honour of Edward Mcwhinney,* Martinus Nijhoff, 2009, p. 455-466.

- KOUZMANOV, K., *NATO's response to the 11 September 2001 terrorism: lessons learned*, Thesis, Naval Postgraduate School, Monterrey, 2003

- KREß, C., "Some reflections on the international legal framework governing transnational armed conflict", *JCSL*, 15, 2010, p. 245-274.

- KRETZMER, D., "The inherent right to self-defense and proportionality in *jus ad bellum*", *EJIL*, 24(1), 2013, p. 235-282.

- KRITSIOTIS, D., "When States use armed force", *Cambridge Studies in International Relations,* 96, 2004, p. 45-79.

- KITTRICH, J., *The right of individual self-defence in Public International Law*, Logos Verlag Berlin, 2008.

- KUNZ, J. L., "Individual and collective self-defence in article 51 of the Charter of the United Nations", *AJIL*, 41(4), 1947, p. 872-879.

- KWAKWA, E., "The use of force by national liberation movements: trends towards a developing norm", *YJIL*, 14(1), 1989, p. 199-212.

- LACHENMANN, F.; WOLFRUM, R. (eds.), *The law of armed conflict and the use of force: the Max Planck Encyclopedia of Public International Law*, 2, OUP, 2017.

- LACHS, M., *The development and general trends of International Law in our time*, Martinus Nijhoff, 1980.

- LARAE-PEREZ, C., "Economic sanctions as a use of force: revaluating the legality of sanctions from an effects-based perspective", *Boston University International Law Journal*, 20(1), 2002, p. 161-188.

- LAUREN, P. G., "Ultimata and coercive diplomacy", *International Studies Quarterly,* 16(2), 1972, p. 131-165.

- LAURSEN, A., "The judgment by the International Court of Justice in the Oil Platforms case", *NJIL*, 73(1), 2004, p. 135-160.

- LAURSEN, A., "The use of force and (the State of) necessity", *VJTL,* 37, 2004, p. 485-526.

- LAUTERPACHT, H., *Recognition in International Law*, CUP, 3, 2012.

- LOBEL, J., "The use of force to respond to terrorism attacks. The bombing of Sudan and Afghanistan", *YJIL*, 1999, p. 537-557.

- LOUKA, E., “Precautionary self-defence and the future of pre-emption in International Law”, in ARSANJANI, M. H.; *et al*. (eds.), *Looking to the future: essay in International Law in honor of Michael Reisman*, Martinus Nijhoff, 2011, p. 951-988.

- LOVELACE, D. (ed.), Terrorism. Commentary on security documents. *The Obama Administration's Second Term National Security Strategy*, 137, OUP, 2015.

- LOWE, V., "Shorter articles, comments, and notes: ‘clear and present danger’: responses to terrorism", *ICLQ,* 54(1), 2005, p. 185-196.

- LEVENFELD, B., "Israel's Counter-Fedayeen tactics in Lebanon: self-defence and reprisal under modern International Law", *Columbia Journal of Transnational Law,* 21(1), 1982, p. 1-48.

- LEVY, J. S., "Preventive war and democratic politics", *International Studies Quarterly*, 52(1), 2008, p. 1-24.

- LIEBLICH, E., *International Law and civil wars: intervention and consent*, Routledge, 2013.

- LOWE, V., “The Iraq crisis: what now?”, *ICLQ*, 52 (4), 2003, p. 859-871.

- LUBELL, N., *Extraterritorial use of force against non-State actors*, OUP, 2010.

- MAGGS, G. E., "The campaign to restrict the right to respond to terrorist attacks in self-defence under article 51 of the UN Charter and what the United States can do about it", *Regent Journal of International L*aw, 4, 2006, p. 149-174.

- MALANTOWICZ, A., “Civil war in Syria and the new wars debate", *Amsterdam Law Forum,* 5(3), 2013, p. 52-60.

- MARAUHN, Th.; NTOUBANDI, Z. F., “Armed conflict, non-international”, in LACHENMANN, F.; WOLFRUM, R. (eds.), *The law armed conflict and the use of force. The Max Planck Encyclopedia of Public International Law,* 2, OUP, 2017, p. 58-70

- MARQUEZ, M. C., *Problemas actuales sobre la prohibicion del recurso a la fuerza en Derecho Internacional*, Tecnos, 1998.

- MARTINEZ, J. M.; URREA, M. (coord), *Seguridad internacional y guerra preventiva: analisis de los nuevos discursos sobre la guerra*, Perla, 2008.

- MARXSEN, C., "Territorial integrity in International Law–its concept and implications for Crimea", *Zeitschrift für Ausländisches,* 75 (1), 2015, p. 7-26.

- MATSUI, Y., “Anticipatory or preemptive self-defence and the world order under the UN Charter”, in DIXIT, R. K.; *et al*. (eds.), *International Law: issues and challenges*, Gurgaon, 2009, p. 139-147.

- McCOUBREY, H.; WHITE, N. D., *International Law and armed conflict*, Dartmouth, 1992.

- McDOUGAL, M. S.; FELICIANO, F. S., *Law and minimum world public order: the legal regulation of international coercion*, Yale University Press, 1961.

- McGUINNESS, M. E., "Case concerning armed activities on the territory of the Congo: the ICJ finds Uganda acted unlawfully and orders reparations", ASILI*,* January 2006, *University of Missouri School of Law Legal Studies Research Paper,* 11, 2009, p. 1-7, available at https://ssrn.com/abstract=1394533, [visited on 21 June 2018].

- McKEEVER, D., "The contribution of the International Court of Justice to the law on the use of force: missed opportunities or unrealistic expectations?", *NJIL*, 78(3), 2009, p. 361-396.

- MENON, P. K., *The law of recognition in International Law. Basic principles,* Edwin Mellen Press*,*1994.

- MILLEN, R. A.; METZ, S., *Insurgency and counterinsurgency in the 21st Century: reconceptualizing threat and response*, Diane Publishing, 2004.

- MILANOVIĆ, M., "State responsibility for acts of non-State actors. A comment on GRIEBEL and PLÜCKEN", *LJIL*, 22(2), 2009, p. 307-324.

- MILOJEVIĆ, M. B., "Prohibition of use of force and threats in international relations", *Teme,* 27(4), 2003, p. 609-637.

- MOMTAZ, J., "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force", *YJIL*, 29(2), 2004, p. 307-313.

- MOORE, J. N., *et al*. (ed.), *Legal issues in the struggle against terror*, Carolina Academic Press, 2010.

- MORI, T., *Origins of the right of self-defence in International Law. From the Caroline incident to the United Nations Charter*, Brill, 2018.

- MURASE, S., "The relationship between the UN Charter and general International Law regarding non-use of force: the case of NATO's air campaign in the Kosovo crisis of 1999, in - ANDO, N; *et al., Liber amicorum judge Shigeru Oda,* Kluwer, 2002, p. 1543-1554.

- MURASE, S., "Unilateral response to International terrorism: self-defence or law enforcement?, in YEE, S.; MORIN, J. (eds.), *Multiculturalism and International Law: essay in honour of Edward Mcwhinney,* Martinus Nijhoff, 2009, p. 429-454.

- MURPHY, S. D., "Terrorism and the concept of 'armed attack' in article 51 of the UN Charter", *HILJ,* 43(1), 2002, p. 42-51.

- MURPHY, S. D., "Assessing the legality of invading Iraq", *Georgetown Law Journal,* 92(2), 2003, p. 173-257.

- MURPHY, S. D., "Self-defence and the Israeli Wall Advisory Opinion: an *ipse dixit* from the ICJ?", *AJIL*, 99(1), 2005, p. 62-76.

- MURPHY, S. D., "The doctrine of preemptive self-defense", *Villanova Law Review,* 50(3), 2005, p. 699-748.

- MURRAY, C. R. J.; O'DONOGHUE, A., "Towards unilateralism? House of Common oversight of the use of force", *ICLQ*, 65(2), 2016, p. 305-341.

- MYERS, M. A., "Deterrence and the threat of force ban: does the UN Charter prohibit some military exercises", *Military Law Review,* 162, 1999, p. 132-179.

- MYJER, E. P. J.; WHITE, N, D., "The twin towers attack: an unlimited right to self-defence?", *JCSL*, 7(1), 2002, p. 5-17.

- NASU, H., *International Law on peacekeeping: a study of article 40 of the UN Charter*, Brill, 2009.

- NEUHOLD, H., Anticipatory self-defence: legal analysis versus strategic realities", *Austrian Review of International and European Law*, 14, 2009, p. 61-78.

- NEUHOLD, H., *The law of international conflict: force, intervention and peaceful dispute settlement*, Brill, 2015.

- NOLTE, G., "Intervention by invitation", in *Max Planck Encyclopedia of Public International Law*, 2010, available at http://opil.ouplaw.com,]visited on 2 July 2017[.

- NOLTE, G.; RANDELZHOFER, A., "Article 51", in SIMMA, B.; *et. al*., (eds.), *The Charter of the United Nations: a commentary,* vol. 2, 3rd ed., OUP, 2012, p. 1397-1428.

- NUNGESSER, D., "United States' use of the doctrine of anticipatory self-defence in Iraqi conflicts", *Pace University School of Law International Law review*, 16, 2004, p. 193-220.

- OBAYEMI, O. K., "Legal standards governing pre-emptive strikes and forcible measures of anticipatory self-defence under the UN Charter and General International Law*", Annual Survey of International Law and Comparative Law*, 12, 2006, p. 19-42.

- OCHOA, R. N.; SALAMANCA-AGUADO, E., "Exploring the limits of International Law relating to the use of force in self-defence", *EJIL*, 16(3), 2005, p. 499-524.

- O'CONNEL, M. E., "Lawful self-defence to terrorism", *University of Pittsburgh Law Review*, 63, 2002, p. 889-908.

- O'CONNELL, M. E., "Evidence of terror", *JCSL*, 7(1), 2002, p. 19-36.

- O'CONNELL, M. E., "The myth of pre-emptive self-defence", *The American Society of International Law*, August 2002, p. 1-21.

- O'CONNELL, M. E., "The legal case against the global war and terrorism", *Case Western Reserve Journal of International Law*, 36(2/3), 2004, p. 349-357.

- O'CONNELL, M. E., "Enhancing the status of non-State actors through a global war on terror", *Columbia Journal of Transnational Law,* 43, 2005, p. 435-458.

- O'CONNELL, M. E., "Rules of evidence for the use of force in International Law's new era", *Proceedings of the Annual Meeting (American Society of International Law),* 100, 2006, p. 39-54.

- O'CONNELL, M. E.; ALVERAS-CHEN, M., "The ban on the bomb-and bombing: Iran, the U.S., and the International Law of self-defence", *Syracuse Law Review*, 57, 2007, p. 497- 517.

- O'CONNELL, M. E., *The power and purpose of International Law*, OUP, 2008.

- O'CONNELL, M. E., "The choice of law against terrorist", *Journal of National Security Law and Policy*, 4, 2010, p. 343-368.

- O'CONNELL, M. E.; MIYAZMATOV, M., "What is aggression? Comparing the *jus ad bellum* and the ICC Statute", *Journal of International Criminal Justice,* 10(1), 2012, p. 189-207.

- O'CONNEL, M. E., "*Jus cogens* , International Law higher ethical norms", in CHILDRESS, D. E. (ed.), *The role of ethic in International Law*, CUP, 2011, p. 78-100.

- O'CONNELL, M. E., "Adhering to law and values against terrorism", Notre Dame Journal of International & Comparative Law*,* 2(2), 2012, p. 289-304.

- O'CONNELL, M. E.; EL MOLLA, R., "The prohibition on the use of force for arms control: the case of Iran nuclear program", *Penn State Journal of Law* & *International Affairs*, 2(2), 2013, p. 315-328.

- O'CONNEL, M. E., "The prohibition of use of force", in WHITE, N. D.; HENDERSON, Ch. (eds.), *Research handbook on international conflict and security law*, Edward Elgar, 2013, p. 89-119.

- ODENDAHL, K., "The scope of application of the principle of territorial integrity", *GYIL*, 53, 2010, p. 511-540.

- OHLIN, J. D.; MAY, L., *Necessity in International Law*, OUP*,* 2016.

- OKIMOTO, C., "The cumulative requirements of *jus ad bellum* and *jus in bello* in the context of self-defence", *Chinese Journal of International Law,* 11, 2012, p. 45-75.

- ORR, A. C., "Unmanned, unprecedented, and unresolved: The status of American drone strikes in Pakistan under International Law", *Cornell International Law Journal*, 44(3), 2011, p. 729-752.

- ORTEGA, M. C., *La legítima defensa del territorio del Estado. Requisitos para su ejercicio*, Tecnos, 1991.

- ÖYKÜIRMAKKESEN, *The notion of armed attack under the UN Charter and the notion of international armed conflict-interrelated or distinct?,* Geneva Academy, 2014.

- PADDEU, F. I., "Self-defence as a circumstance precluding wrongfulness: understanding article 21 of the article on State responsibility", *BYIL*, 85, 2014, p. 90-132.

- PALCHETTI, P., "Customary rules on the use of force in the work of codification of the International Law Commission", in CANNIZZARO, E.; PALCHETTI, P., *Customary International Law on the use of force: a methological approach*, Martinus Nijhoff, 2005, p. 233-241.

- PALMISANO, G., "Determining the law on the use of force: the ICJ and customary rules on the use of force", in CANNIZZARO, E.; PALCHETTI, P., *Customary International Law on the use of force: a methological approach*, Martinus Nijhoff, 2005, p. 197-218.

- PASTOR, J. A., *Curso de Derecho Internacional Público y organizaciones internacionales*, 22nd ed., Tecnos, 2018.

- PAUST, J. J., "Use of armed force against terrorists in Afghanistan, Iraq, and beyond", *Cornell International Law Journal,* 35(3), 2002, p. 533-557.

- PAUST, J. J., "Self-defense targeting of non-State actors and permissibility of US use of drones in Pakistan", *Journal of Transnational Law and Policy*, 19(2), 2009, p. 237-279.

- PELLET, A., "Les articles de la C.D.I. sur la responsabilité de l'Etat pour fait internationalement illicite. Suite-et fin?", *AFDI,* 48, 2002, p. 1-23.

- PÉREZ, E., *Naciones Unidas y los principios de coexistencia pacífica*, Tecnos, 1973.

- PÉREZ, M., "La legítima defensa puesta en su sitio: observaciones críticas sobre la doctrina Bush de la acción preventiva", *REDI*, 55 (1), 2003, p. 187-204.

- PERT, A., "Proportionality in self-defence–proportionate to what?", *Pandora Box*, 24(17/95), 2017, p. 65-78.

- PETERS, A., "German Parliament decides to send troops to combat ISIS, based on collective self-defence in conjunction with SC 2249", *EJIL Talk*, December 2015, available at http://www.ejiltalk.org,]visited on 21 June 2018[.

- PIÑOL, J., *El principio de no intervención*, Doctoral thesis unpublished, UAB, 1978.

- PIÑOL, J., "Los asuntos de las actividades militares y paramilitares en Nicaragua y en contra de este Estado(Nicaragua contra Estados Unidos de America), *REDI*, 39(1), 1987, p. 99-120.

- PLANT, R., "Rights, rules and world order", in DESAI, M.; REDFERN, P. (eds.), *Global governance: ethics and economics of the world order*, Pinter, 1995, p. 190-218.

- POZO, P., "La Carta de las Naciones Unidas y el régimen jurídico del uso de la fuerza: algunos problemas de interpretacion", *Revista del Instituto Espanol de Estudios Estrategicos*, 1, 2013, p. 1-28.

- PRINTER, N. G., "Use of force against non-State actors under International Law: an analysis of the US predator strike in Yemen", *UCLA Journal of International Law & Foreign Affairs,* 8, 2003, p. 331-383.

- QUOC DINH, N., "La légitime défense d'après la Charte des Nations Unies", *RGDIP*, 52, 1948, p. 223-254.

- RAAB, D., "Armed attack after the Oil Platform case", *LJIL,* 17, 2004, p. 719-735.

- RABY, J., "The State of necessity and the use of force to protect Nationals", *CYIL,* 26, 1989, p. 253-272.

- RAMON, C. (coord)., *La acción colectiva del uso de la fuerza. Nuevos scenarios, nuevos principios de actuación en el orden internacional,* Tirant lo Blanch, 2012.

- RANDELZHOFER, A.; DÖRR, O., "Article 2(4)", in SIMMA, B., *et al*. (ed.), *The Charter of the United Nations. A Commentary,* vol. 1, 3rd ed., OUP, 2012, p. 200-234.

- RAO, P. S., "Non-State actors and self-defence: a relook at the UN Charter article 51", *Indian Journal of International Law*, 56(2), 2016, p. 127-171.

- RATNER, S. R,. "*Jus ad bellum* and *jus in bello* after September 11", *AJIL*, 96(4), 2002, p. 905-921.

- RATNER, S. R., "Self-defence against terrorists: the meaning of armed attack", *MJIL*, 2012, p. 1-20.

- REINOLD, T., "State weakness, irregular warfare, and right to self-defence post 9/11", *AJIL*, 105(2), 2011, p. 244-286.

- REISMAN, W. M., "Coercion and self-determination: construing Charter article 2(4)", *AJIL,* 78(3), 1984, p. 642-645.

- REISMAN, W. M.; ARMSTRONG, A., "The past and future of the claim of pre-emptive self-defence, *AJIL*, 100(3), 2006, p. 525-550.

- REMIRO, A.; *et al*., *Derecho Internacional*, Tirant lo Blanch, 2010.

- RIDDELL, A.; PLANT, B., *Evidence before the International Court of Justice*, British Institute of International and Comparative Law, 2009.

- RIPOL, S., "La nueva doctrina global de la defensa preventiva. Consideraciones sobre su caracterización y fundamento", in GARCIA, C., RODRIGO, A. (eds.), *El imperio inviable. El orden internacional tras el conflicto de Irak*, Tecnos, 2005.

- RISEN, J., “Question of evidence: a special report. To bomb Sudan Plant, or not: a year later, debates rankle”, *New York Times*, 27 October 1999.

- RISHIKOF, H., "When naked came the doctrine of self-defence: what is the proper role of the International Court of Justice in use of force cases", *YJIL,* 29, 2004, p. 331-342

- ROBERTS, G. B., "Self-help in combating State-sponsored terrorism: self-defence and peacetime reprisals", *Case Western Reserve Journal of International Law***,** 19, 1987, p. 243-293.

- ROBERTS, G. B., "The counterproliferation self-help paradigm: a legal regime for enforcing the norm prohibiting the proliferation of weapons of mass destruction", *Denver Journal of International Law & Policy,* 27(3), 1998, p. 483-518.

- ROBERTSON, H. B., "Self-defense against computer network attack under International Law", in SCHMITT, M. N.; O’DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002, p. 121-145.

- RÖLING, B. V. A., “Aspects of the ban on force”, *NILR,* 24, 1977, p. 242-259.

- RÖLING, B. V. A., “The ban on the use of force and the UN Charter”, in CASSESE, A., *The current legal regulation of the use of force,* Martinus Nijhoff, 1986, p. 3-9.

- RONZITTI, N., *Rescuing nationals abroad through military coercion and intervention on grounds of humanity*, Martinus Nijhoff , 1985.

- RONZITTI, N., “The current status of legal principles prohibiting the use of force and legal justifications of the use of force”, in BOTHE, M.; O’CONNELL, M. E. (eds.)*, Redefining sovereignty: the use of force after the cold war*, Ardsley, 2005, p. 91-110.

- RONZITTI, N., "The expanding law of self-defence", *JCSL*, 11(3), 2006, p. 343-359.

- ROSAND, E., “Security Council Resolution 1373, the Courter–terrorism Committee and the fight against terrorism”, *AJIL*, 97(2), 2003, p. 333-341.

- ROSCINI, M., "Threats of armed force and contemporary International Law", *NILR*, 54(2), 2007, p. 229-277.

- ROSTOW, E. V., “Until what? Enforcement action or collective self-defence?”, *AJIL*, 85(3), 1991, p. 506-516.

- ROSTOW, N., “International Law and the use of force: a plea for realism”, *YJIL*, 34(2), 2009, p. 549-557.

- ROTHWELL, D., “Anticipatory self-defence in the age of international terrorism”, *The University of Queensland Law Journal*, 24(2), 2005, p. 337-353.

- ROUCOUNAS, E., "Problèmes actuels du recours à la force en Droit International", *Annuaire de l'Institut de Droit International*, 72(1), 2007, p. 75-159.

- RUYS, T.; VERHOEVEN, S., "Attacks by private actors and the right of self-defence", *JCSL*, 10(3), 2005, p. 289-320.

- RUYS, T., "*Quo vadit jus ad bellum*?: a legal analysis of Turkey's military operation against the PKK in Northern Iraq", *Melbourne Journal of International Law*, 9(2), 2008, p. 334-363.

- RUYS, T., "The protection of nationals doctrine revisited", *JCSL*, 13, 2008, p. 233-271.

- RUYS, T., *'Armed attack' and article 51 of the UN Charter. Evolutions in customary law and practice,* CUP, 2010.

- RUYS, T., "The meaning of 'force' and the boundaries of the *jus ad bellum*: are 'minimal' use of force excluded from UN Charter article 2(4)?", *AJIL*, 108(2), 2014, p. 159-210.

- RUYS, T.; *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018.

- SADOFF, D. A. A., "Question of determinacy: the legal status of anticipatory self-defence", *Georgetown Journal of International Law*, 40(2), 2009, p. 523-576.

- SADOFF, D. A. A., "Striking a sensible balance on the legality of defensive first strikes", *VJTL*, 42, 2009, p. 441-500.

- SADURSKA, R., "Threat of force", *AJIL,* 82(2), 1988, p. 239-268.

- SALINAS, A. M., "Lucha contra terrorismo internacional: no solo del uso de la fuerza pueden vivir los Estados", *REDI*, 68(2), 2016, p. 229-252.

SAMPSON, E., "Necessity, proportionality and distinction in nontraditional conflicts" in FORD, C. A.; COHEN, A. (eds.), *Rethinking the law of armed conflict in an age of terrorism*, Lexington Books, 2012, p. 195-214.

- SÁNCHEZ, L. I., "Una cara oscura del Derecho Internacional: legítima defensa y terrorismo internacional", *Cursos de Derecho Internacional de Vitoria-Gasteiz 2002,* Universidad del País Vasco, 2004, p. 269-299.

- SANJOSE, A, "La legítima defensa individual y colectiva y el artículo 51 de la Carta de las Naciones Unidas", in CARDONA, J. (ed.), La ONU y el mantenimiento de la paz en el siglo XXI: entre la adaptación y la reforma de la Carta, Tirant lo Blanch, 2008, p.

- SAPIRO, M., "Pre-empting prevention: lessons learned", *New York University Journal of International Law and Politics*, 37(2), 2005, p. 357-371.

- SARVARIAN, A., "The lawfulness of a use of force upon nuclear facilities in self-defence", *JUFIL*, 1(2), 2014, p. 247-272.

- SAURA, J., “Some remarks on the use of force against terrorism in contemporary International Law and the role of Security Council”, *Loyola Los Angeles International & Comparative Law Review,* 26 (1), 2003, p. 7-30.

- SAYAPIN, S., *The crime of aggression in international criminal law: historical development, comparative analysis and present State*, Springer Science & Business Media, 2014.

- SAYAPIN, S., “International Law on the use of force: current challenges”, available at http://www.academia.edu/25835283/International_Law_on_the_Use_of_Force_Current_Challenges,]visited on 20 June 2018[.

- SCHACHTER, O., “The right of States to use armed force”, *Michigan Law Review*, 82, 1984, p. 1620-1646.

- SCHACHTER, O., “In defense of international rules on the use of force”, *University of Chicago Law Review*, 53(1), 1986, p. 113-146.

- SCHACHTER, O., '' Self-defense and the rule of law'', *AJIL,* 83(2), 1989, p. 259-277.

- SCHACHTER, O., “The use of force against terrorists in another country”, *Israel Yearbook on Human Rights*, 19, 1989, p. 209-231.

- SCHINDLER, D., *The different types of armed conflicts according to the Geneva Conventions and Protocols*, Martinus Nijhoff, 1979.

- SCHMIDL, M., *The changing nature of self-defence in International Law*, Nomos, 2009.

- SCHMITT, M. N., *Counter –terrorism and the use of force in International Law*, The George C. Marshall European Center for Security Studies, The Marshal Center Papers, 5, 2002.

- SCHMITT, M. N., "Pre-emptive strategies in International Law", *MJIL,* 24(2), 2003, p. 513-548.

- SCHMITT, M. N.; PEJIC, J. (eds.), *International Law and armed conflict: exploring the faultlines*, Brill, 2007.

- SCHMITT, M. N., "Drone attacks under the *jus ad bellum* and *jus in bello*: clearing the ‘fog of law’", *Yearbook of International Humanitarian Law,* 13, 2010, p. 311-326.

- SCHMITT, M. N., *Essays on law and war at the fault lines*, Springer Science & Business Media, 2011.

- SCHRIJVER, N., “Responding to international terrorism: moving the frontiers of International Law for ‘enduring freedoms’”, *NILR*, 48(3), 2001, p. 271-291.

- SCHRIJVER, N., “The use of force under the UN Charter: restrictions and loopholes”*, Memorial lecture delivered at John W. Holmes,* retrieved on 7 November*,* 2003, available at

https://acuns.org/wp-content/uploads/2012/09/WebPageSchrijver_UseofForce.pdf, [visited on 21 June 2018].

- SCHRIJVER, N., "Challenges to the prohibition to use of force: does the straitjacket of article 2(4) UN Charter begin to gall too much?", in BLOKKER, N.; SCHRIJVER, N. (eds.*), The Security Council and the use of force theory and reality-a need for change?*, Martinus Nijhoff, 2005, p. 31-45.

- SCHRIJVER, N.*,* "The future of the Charter of the United Nations", *Max Planck Yearbook of United Nations Law,* 10, 2006, p. 1-34.

- SCHRIJVER, N., "The ban on the use of force in the UN Charter", in WELLER, M.; *et al.* (eds.), *The Oxford handbook of the use of force in International Law,* OUP, 2015, p. 465-487.

- SCHWEBEL, S. M., "Aggression, intervention and self-defense in modern International Law", *RCADI*, 136 (2), 1972, p. 411-497.

- SEELOS, B., *The Anti-secession law and the use of threat - is China`s policy towards Taiwan a violation of art 2 (4) UN Charter?,* Diplomarbeit, 2009.

- SENN, M.; TROY, J., "The transformation of targeted killing and international order", *Contemporary Security Policy*, 38(2), 2017, p. 175-211.

- SERRANO, R., "EL terrorismo y el Derecho Internacional", *Anuario Mexicano de Derecho Internacional*, 3, 2003, p. 353-373.

- SHAH, S. A., "War on terrorism: self defense, operation enduring freedom, and the legality of US drone attacks in Pakistan", Washington University Global Studies Law Review*,* 9(1), 2010, p. 77-129.

- SHAH, N. A., "Self-defence, anticipatory self-defence and pre-emption: International Law's response to terrorism", *JCSL,* 12(1), 2007, p. 95-126.

- SHAH, N. A., "The use of force under Islamic Law", *EJIL*, 24(1), 2013, p. 343-365.

- SHANY, Y., "The analogy's limit: defending the rights of peoples", *Journal of International Criminal Justice*, 7(3), 2009, p. 541-553.

- SICILIANOS, L. A., *Les réactions décentralisées à l'illicite: des contre-mesures à la légitime défense*, Université Robert Schuman, 1990.

- SILVER, D. B., "Computer network attack as a use of force under article 2(4) of the United Nations Charter", in SCHMITT, M. N.; O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002, p. 74-97.

- SIMMA, B., "NATO, the UN and the use of force: legal aspects", *EJIL,* 10(1), 1999, p. 1-22.

- SINGH, J. N., *Use of force under International Law*, Harnam, 1984.

- SOFAER, A. D., "International security and the use of force", in MILLER, R. A.; BRATSPIES, R. M., *Progress in International Law,* Martinus Nifhoff, 2008, p. 539–570.

- SONNENFELD, R, *Resolutions of the United Nations Security Council*, Martinus Nijhoff, 1988.

- SORENSEN, M., *Manual of Public International Law*, Mac Millan, 1968.

- SPEROTTO, F., "The use of force against terrorism: a reply to Christian J. Tams", *EJIL,* 20(4), 2009, p. 1043-1048.

- SREENIVASA, R. P., "International Organizations and use of force", in ANDO, N.; *et al., Liber amicorum judge Shigeru Oda,* Kluwer, 2002, p. 1575-1608.

- STAHN, C., "Terrorist acts as 'armed attack': the right to self-defence, article 51(1/2) of the UN Charter, and international terrorism", *Fletcher Forum of World Affairs*, 27, 2003, p. 35-54.

- STAHN, C., "'Nicaragua is dead, long live Nicaragua'- the Right to Self-defence under Art. 51 UN-Charter and international terrorism", in WALTER, C.; *et al*. (eds.), *Terrorism as a challenge for national and International Law: security versus liberty?*, Springer, 2004, p. 827-877.

- STARSKI, P., "Right to self-defence, attribution and the non-State actor–birth of the 'unable and unwilling' standard?", *Heidelberg Journal of International Law,* 75, 2015, p. 455-501.

- STROMSETH, J. E., "Law and force after Iraq: a transitional moment", *AJIL*, 97(3), 2003, p. 628-642.

- STÜRCHLER, N., *The threat of force in International Law*, CUP, 53, 2007.

- STURMA, P., "Enforcing international obligations through the use of force", *Revue Hellenique de Droit International,* 61, 2008, p. 595-631.

- SUTTERLIN, J. S., *The United Nations and the maintenance of international security: a challenge to be met*, Greenwood, 2003.

- SZABÓ, K. T., *Anticipatory action in self-defence. Essence and limits under International Law*, Springer Science & Business Media, 2011.

- TAMS, C. J., "Light treatment of a complex problem: the law of self-defence in the Wall case", *EJIL*, 2005, 16(5), p. 963-978.

- TAMS, C. J., "Swimming with the tide or seeking to stem it? Recent ICJ ruling on the law on self-defence", *Revue Quebecoise de Droit International*, 18, 2005, p. 275-290.

- TAMS, C. J., "The use of force against terrorists"*, EJIL,* 20(2), 2009, p. 359-395.

- TAMS, C. J.; DEVANEY, J. G., "Applying necessity and proportionality to anti-terrorist self-defense", *Israel Law Review,* 45(1), 2012, p. 91-106.

- TAMS, C. J.; SLOAN, J.*, The development of International Law by the International Court of Justice*, OUP, 2013.

- TANCREDI, A., "Secession and use of force", in WALTER, C.; *et al*. (eds.), *Self-determination and session in International Law*, OUP, 2014, p. 68-94.

- TERRY, P. C. R.; OPENSHAW, K. S., "Nuclear non-proliferation and 'preventive self-defence'; why attacking Iran would be illegal", *CYIL*, 51, 2013, p. 165-215.

- THOMSON, A. W. R., "Doctrine of the protection of nationals abroad: rise of the non-combatant evacuation operation", *Washington University Global Studies Law Review*, 11(3), 2012, p. 627-668.

- THOUVENIN, J. M., "Circumstances precluding wrongfulness in the ILC article on state responsibility: self-defence", in CRAWFORD, J., *et. al*. (eds.), *The law of international responsibility*, OUP, 2010, p. 455-468.

- TOMAS, C.; BRUCKNER, W., "The Israeli intervention in Lebanon-2006", in RUYS, T., *et al*., *The use of force in International Law. A case-based approach*, OUP, 2018, p. 673-688.

- TOMUSCHAT, CH. (ed.), *Modern law and self-determination*, Martinus Nijhoff, 16, 1993.

- TOMUSCHAT, C., "Secession and self-defence", in KOHEN, M. G. (ed.), *Secession: International Law perspectives,* CUP, 2006, p. 23-45.

- TOTTEN, M., "Using force first: moral tradition and the case for revision", *Stanford Journal of International Law*, 43(1), 2007, p. 95-126.

- TRAPP, K. N., "Back to basic: necessity, proportionality, and the right of self-defence against non-State terrorist actors", *ICLQ,* 56(1), 2007, p. 141-156.

- TRAPP, K. N., *State responsibility for international terrorism*, OUP, 2011.

- TRAPP, K. N., "Can non-State actors mount to an armed attack", in WELLER, M.; *et al*. (eds.), *The Oxford handbook of the use of force in International Law*, CUP, 2015, p. 679-696.

- TRAPP, K. N., "Terrorism and the Internantional Law of State responsibility", in SAUL, B. (ed.), *Research Handbook on International Law and terrorism*, Edward Elgar, 2014, p. 39-56.

- TRAPP, K. N., "The Turkish intervention against the PKK in Northern Iraq-2007-08", in RUYS, T.; *et al*. (eds.), *The use of force in International Law. A case-based approach*, OUP, 2018, p. 689-701.

- TREVEZ, T., "La Déclaration des Nations Unies sur le renforcement de l'efficacité du principe de non-recours à la force", *AFDI*, 33, 1987, p. 379-398.

- TSAGOURIAS, N., "Necessity and the use of force: a special regime", in *Necessity across International Law, NYIL*, 41, 2010, p. 11-44.

- TSAGOURIAS, N., "Non-State actors in international institutional peace and security: non-State actors and the use of force", in D'ASPREMONT, J. (ed.) *Participants in the international legal system: multiple perspectives on non-State actors in International Law,* Roudledge, 2011, p. 326-341.

- TSAGOURIAS, N., "The prohibition of threats of force", 2012, available at http://ssrn.com/abstract=2074015,]visited on 21 June 2018[.

- TSAGOURIAS, N., "The prohibition of threats of force", in WHITE, N. D.; HENDERSON, Ch. (eds.), *Research handbook on international conflict and security law*, Edward Elgar, 2013, p. 67-88.

- VACAS, F., *El régimen jurídico del uso de la fuerza por parte de las operaciones de mantenimiento de la paz de Naciones Unidas*, Universidad Carlos III, 2005.

- VALLARTA, J. L., "El derecho inmanente a la legítima defensa individual o colectiva en caso de ataque armado ¿se justifica una interpretación extensiva para incluir medidas preventivas y punitivas? Una visión Israelí*", Anuario Mexicano de Derecho Internacional, 9*, 2009, p. 69-115.

- VAN DE HOLE, L., "Anticipatory self-defence under International Law", *American University International Law Review*, 19(1), 2003, p. 69-106.

- VAN DEN HERIK, L.; SCHRIJVER, N. (eds.), *Counter-terrorism strategies in a fragmented international legal order. Meeting the challenges*, CUP, 2013.

- VAN STEENBERGHE, R., "Self-defence in response to attacks by non-State actors in the light of recent State practice: a step forward?", *LJIL,* 23(1), 2010, p. 183-208.

- VERDROSS, A.; SIMMA, B., "Universelles Völkerrecht. Theorie und Praxis", *VRÜ Verfassung und Recht in Übersee,* 11(1), 1977, p. 128-130.

- VERHOEVEN, J., "Les «étirements» de la légitime défense", *AFDI*, 48, 2002, p. 49-80.

- VILLANI, U., "The Security Council's authorization of enforcement action by regional organizations", *Max Planck Yearbook of United Nations Law online,* 6(1), 2002, p. 535-555, available at http://booksandjournals.brillonline.com/content/journals/10.1163/138946302775159352,]visited on 25 June 2018[.

- VITE, S., "Typology of armed conflicts in International Humanitarian Law: legal concepts and actual situations", *International Review of the Red Cross,* 91(873), 2009, p. 69-94.

- VITKOWSKY, V. J., "Remarks on customary International Law and the use of force against terrorists and rogue State collaborators", *ILSA Journal of International and Comparative Law*, 13(2), 2007, p. 371-378.

- WALDOCK, C. H. M., "*L'interdiction du recours à la force: le principe et les problèmes qui se posent*", *RCADI*, 78(1), 1951, p. 1-122.

- WALDOCK, C. H. M., "The regulation of the use of force by individual States in International Law", *RCADI*, 81(2), 1952, p. 451-517.

- WALZER, M., *Just and unjust wars: a moral argument with historical illustrations*, 5th ed., Basic Books, 2015.

- WAXMAN, M. C., Regulating resort to force: form and substance of the UN Charter regime, *EJIL*, 24, 2013, p. 151-189.

- WEDGWOOD, R., "Responding to terrorism: the strikes against Bin laden", *YJIL*, 24, 1999, p. 559-576.

- WEDGWOOD, R., "NATO's campaign in Yugoslavia", *AJIL*, 93(4), 1999, p. 828-834.

- WEDGWOOD, R., "The ICJ Advisor Opinion on the Israeli security fence and the limits of the self-defence", *AJIL*, 99(1), 2005, p. 52-62.

- WESTRA, J. H., *International Law and the use of armed force: the UN Charter and the major powers*, Routledge, 2007.

- WETTBERG, G., *The international legality of self-defence against non-State actors: State pactice from the UN Charter to the present*, Peter Lang, 2007.

- WHITE, N. D.; CRYER, R., "Unilateral enforcement of Resolution 687: a threat too far?", *California Western International Law Journal,* 29(2), 1999, p. 243-282.

- WILLIAMS, G.D., "Piercing the shield of sovereignty: an assessment of the legal status of the 'unwiling or unable' test", *University of New South Wales Law Journal,* 36(2), 2013, p. 619-641.

- WILMHURST, E.; WOOD, M., "Self-defence against non-State actors: reflections on the 'Bethlehem Principles'", *AJIL*, 107(2), 2013, p. 390-395.

- WILSON, R. R., "Recognition of insurgency and belligerency", *American Society of International Law Proceedings*, 31, 1937, p. 136-143.

- WILSON, H. A., *International Law and the use of force by national liberation movements*, OUP, 1999.

- WILSON, G., "The impact of 9/11 on the use of force in the International Law: ten years on", in UTLEY, R. E., (ed.), *9/11 ten years after: perspectives and problems*, Routledge, 2012, p. 179-195.

- WIPPMAN, D., "The nine lives of article 2(4)", *Minnesota Journal of International Law*, 16(2), 2007, p. 387-403.

- WITTICH, S., "The use of force, self-defence and the unrealism in International Law", *Austrian Review of International and European Law*, 14, 2009, p. 79-102.

- WLAŹ, A., "Preclusion of wrongfulness of the use of force", *International Community Law Review*, 13(1-2), (2011), p. 125-146.

- WOOD, M., "International Law and the use of force: what happens in practice", *Indian Journal of International Law*, 53, 2013, p. 346-367.

- WRACHFORD, J. S., "The 2006 Israel invasion of Lebanon: aggression, self-defence, or a reprisal gone bad?", *Air Force Law Review*, 60, 2007, p. 29-75.

- YUSUF, A. A., "The notion of armed attack in the Nicaragua judgment and its influence on subsequent case law", *LJIL*, 25(2), 2012, p. 461-470.

- ZAYAC, R. A., "'United States' authority to legally implement the self-defence and anticipatory self-defence doctrines to eradicate the threat posed by countries harbouring terrorists and producing weapons of mass destruction", *Southern Illinois University Law Journal*, 29, 2004, p. 433-455.

- ZEDALIS, R. J., "Protection of nationals abroad: is consent the basis of legal obligation?", *Texas International Law Journal*, 25, 1990, p. 209-270.

- ZEMANEK, K., "Self-defense against terrorism; reflections on an unprecedented situation", in MARIÑO, F. (coord.), *El Derecho Internacional en los albores del siglo XXI. Homenaje al profesor Juan Manuel Castro-Rial Canosa*, Trotta, 2002, p. 695-714.

- ZEMANEK, K., "The prohibition to use force after sixty years of abuse", in BUFFARD, I.; *et al*. (eds.), *International Law between universalism and fragmentation: in honour of Gerhard Hafner*, Martinus Nijhoff, 2008, p. 287-316.

- ZEMANEK, K., "Armed attack", in *Max Planck Encyclopedia of Public International Law*, 2013, available at http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241, [visited on 22 June 2018].

B. **The right of self-defence against cyber operations**

ADDDICOTT, J. F., "Cyberterrorism: legal policy issues", in MOORE, J. N., *et al*. (eds.), *Legal issues in the struggle against terror*, Carolina Academic Press, 2010, p. 519-566.

-ALBRIGHT, D.; *et al*., *Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?*, Institute for Science and International Security, 22 December 2010, available at http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf, [visited on August 2017].

- ALLHOFF, F.; *et al.* (eds.), *Binary bullets. The ethics of cyberwarfare*, OUP, 2016.

- ANTOLIN-JENKINS, V. M., "Defining the parameters of cyber war operations: looking for law in all the wrong places", *Naval Law Review,* 51, 2005, p. 132-140.

APPLEGATE S. D., "The principle of maneuver in cyber operations", in CZOSSECK C., *et al.* (eds.), *2012 4th International Conference on Cyber Conflict* (CYCON 2012), NATO CCD COE, 2012, p. 183-195.

- BARKHAM, J., "Information warfare and International Law on the use of force", New York University Journal of International Law and Politics, 34, 2001, p. 57-97.

- BANKS, W., "State responsibility and attribution of cyber intrusion after Tallinn*", Texas Law Review*, 95(7), 2017, p. 1487-1513.

- BLANK, L, R., "International Law and cyber threats from non-State actors", *International Law Studies*, 89, 2013, p. 406-437, at p. 437.

- BOEBERT, E., "A survey of challenges in attribution", in NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, *Proceedings of a workshop on deterring cyber attacks. Informing strategies and developing options for U.S. Policy*, The National Academies Press, 2010, p. 41-55.

- BROWN, D., "A proposal for an international convention to regulate the use of information systems in armed conflict", *HILJ,* 47(1), 2006, p. 179-221.

- BRENNER, S. W., "Cybercrime, cyberterrorism and cyberwarfare", *Revue Internationale de Droit Penal,* 77(3), 2006, p. 453-471.

- BRENNER, S. W., "'At light speed': attribution and response to cyber crime/terrorism/ warfare", *Journal of Criminal Law and Criminology*, 97, 2007, p. 379-475.

- BRENNER, J., *America the vulnerable: inside the new threat matrix of digital espionage, crime, and warfare*, Penguin, 2011.

- BRUNNEE, J.; MESHEL, T., “Teaching an old law new tricks: International Environmental Law lessons for cyberspace governance”, *GYIL,* 58, 2015, p. 129-168.

- BUCHAN, R., "Cyber attacks: unlawful uses of force or prohibited interventions?", *JCSL* 17(2), 2012, p. 211-227.

- CARR, J., *Inside cyber warfare: mapping the cyber underworld*, O'Reilly Media, 2011.

- CARRAPICO, H.; BARRINHA, A., “European Union cyber security as an emerging research and policy field”, *European Politics and Society*, 19(3), 2018, p. 299-303, available at https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430712, [visited on 8 June 2018].

- CONDRON, S. M., "Getting it right: protecting American critical infrastructure in cyberspace", *Harvard Journal of Law and Technology,* 20(2), 2006, p. 403-422.

- CROOK, J. R., “US efforts to enhance cybersecurity and to counter international theft of trade secrets”, *AJIC*, 107(2), 2013, p 447-449.

- CLARK, D. D.; LANDAU, S., “Untangling attribution”, in NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, *Proceedings of a workshop on deterring cyber attacks. Informing strategies and developing options for U.S Policy*, The National Academies Press, 2010, p. 25-40.

- CLARKE, R. A.; KNAKE, R. K., *Cyber war. The next threat to national security and what to do about it*, Harper Collins e-books, 2014, available athttp://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf, [visited on 8 June 2018].

- CHIEN, E., “Stuxnet: a breakthrough, Symantec Blog”, 12 November 2010, available at https://www.symantec.com/connect/blogs/stuxnet-breakthrough, [visited on 22 June 2018].

- DECOULARE-DELAFONTAINE, N., “Cyber attacks on nuclear facilities and nuclear responses to cyber attacks in International Law”, December 17, 2015, p. 1-35, available at http://lcnp.org/pubs/studentpapers/2016/Cyber%20Attacks%20-%20Nina.pdf, [visited 22 June 2018].

- D’ASPREMONT, J., "Cyber operations and International Law: an interventionist legal thought", *JCSL,* 21(3), 2016, p. 575-593.

- DE BORCHGRAVE, A.; *et al*., *Cyber threats and information security: meeting the 21st Century challenge*, Center for Strategic & International Studies, 2001.

- DELIBASIS, D., *The right to national self-defense in information warfare operations*, Arena Books, 2007.

- DEV, P. R., "Use of force and armed attack thresholds in cyber conflict: the looming definitional gaps and the growing need for formal UN response", *Texas International Law Journal,* 50(2), 2015, p. 381-401.

- DEVER, J.; DEVER, J., "Cyber warfare: attribution, preemption, and national self defense", *Journal of Law & Cyber Warfare,* 2(1), 2013, p. 25-63.

- DEWEESE, G. S., "Anticipatory and preemptive self-defense in cyberspace: the challenge of imminence", in MAYBAUM, M., *et al*., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace,* NATO CCD COE, 2015, p. 81-91.

- DINNISS, H. H., *Cyber warfare and the laws of war*, CUP, 92, 2012.

- DINSTEIN, Y., "Computer network attacks and self-defense", in SCHMITT, M. N.; O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002, p. 99-119.

- DINSTEIN, Y., "The principle of distinction and cyber war in international armed conflicts", *JCSL,* 17(2), 2012, p. 261-277.

- DOMINGUEZ, J., "La ciberseguridad: aspectos jurídicos internacionales", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2014*, Aranzadi, 2015, p. 161-223.

- DÖRR, O., "Obligation of the State of origin of a cyber security incident", *GYIL*, 58, 2015, p. 87-99.

- DROEGE, C., "No legal vacuum in cyber space*",* 16 August 2011, available at https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, [visited on 25 April 2017].

- DUCHEINE, P.; *et al*. (eds.), "Towards a legal framework for military cyber operations", *ARMS Netherlands Annual Review of Military Studies*, 2012, p. 101-128.

- DUNLAP, C. J., "Perspectives for cyber strategists on law for cyberwar", *Strategic Studies Quarterly*, 5, 2011, p. 81-99.

- CHRISTIAN, "Israel adds cyber-attack to IDF", 10 February 2010, available at https://www.military.com/defensetech/2010/02/11/israel-adds-cyber-attack-to-idf, [visited on 22 May 2018].

- FOCARELLI, C., "Self-defence in cyberspace", in TSAGOURIAS, N.; BUCHAN, R. (eds.), *Research handbook on International Law and cyberspace.* Edward Elgar, 2015, p. 255-283.

- GARNETT, R.; CLARKE, P., “Cyberterrorism: a new challenge for International Law”, in BIANCHI, A., *Enforcing international law norms against terrorist*, Hart, 2004, p. 465-488.

- GORDON, S.; RICHARD, F. "On the definition and classification of cybercrime", *Journal in Computer Virology,* 2(1), 2006, p. 13-20.

- GOLDSMITH, J., "The new vulnerability", *The New Republic,* 7 June 2010, available at https://newrepublic.com/article/75262/the-new-vulnerability,]visited on 22 June 2018[.

- GRAHAM, D. E., "Cyber threats and the law of war”, *Journal of National Security Law & Policy*, 4, 2010, p. 87-96.

- GREEN, J. A., "Marco Roscini, cyber operations and the use of force in International Law", *JUFIL*, 1(2), 2014, p. 387-394.

- GRIMAL, F.; SUNDARAM, J., “Cyber warfare and autonomous self-defence”, *JUFIL*, 4(2), 2017, p. 312-343.

- GROSSWALD, L., “Cyberattack attribution matters under article 51 of the UN Charter”, *Brooklyn Journal of International Law,* 36(3), 2011, p. 1151-1180.

- GILL, T. D; DUCHEINE, P. A. L., “Anticipatory self-defence in the cyber context”, *International Law Studies*, 89, 2013, p. 438-471.

- GEISS, R.; LAHMANN, H., “Cyber warfare: applying the principle of distinction in an interconnected space”, *Israel Law Review*, 45(3), 2012, p. 381-399.

- GERVAIS, M., "Cyber attacks and the laws of war", *Berkeley Journal of International Law,* 30(2), 2012, p. 525-579.

- GJELTEN, T., "Extending the law of war to cyberspace", 22 September 2010, available at https://www.npr.org/templates/story/story.php?storyId=130023318, [visited on 22 June 2018].

- GLENNY, M., "In America’s new cyberwar google is on the front line", *The Guardian,* 18 January 2010, available at https://www.theguardian.com/commentisfree/2010/jan/18/america-cyberwar-google-china-computer,]visited on 22 June 2018[.

- HATHAWAY, O. A.; *et al*., “The law of cyber-attack”, *California Law Review*, 100(4), 2012, p. 817-885.

- HADJI-JANEV, M.; ALEKSOSKI, S., “Use of force in self-defense against cyber-attacks and the shockwaves in the legal community: one more reason for holistic legal approach to cyberspace”, *Mediterranean Journal of Social Sciences*, 4(14), 2013, p. 115-124.

- HADJI- JANEV, M., “Information legal aspects of protecting civilians and their property in the future cyber conflict”, in INFORMATION RESOURCES MANAGEMENT ASSOCIATION

(ed.), *Cyber security and threats: concept, methodologies, tools, and applications*, IGI Global, 2018, p. 1555-1583.

- HANDLER, S. G., "New cyber face of battle: developing a legal approach to accommodate emerging trends in warfare", *Stanford Journal of International* Law, 48, 2012, p. 209-238, at p. 226-227.

- HERDEGAN, M., "Possible legal framework and regulatory models for cyberspace: due diligence obligations and institutional models for enhanced inter-State cooperation", *GYIL*, 58, 2015, p. 169-185.

- HILDRETH, S. A., *Cyberwarfare*, CRS Report for Congress, updated June 19 2001, available at file:///C:/Users/hamed/Downloads/ADA398642%20(1).pdf, [visited on 22 June 2018}.

- HINKLE, K. C., "Countermeasures in the cyber context: one more thing to worry about", *YJIL*, 37, 2011, p. 11-21.

- HOISINGTON, M., "Cyberwarfare and the use of force giving rise to the right of self-defense", *Boston College International and Comparative Law Review*, 32(2), 2009, p. 439-454.

- HOLLIS, D. B. "Why States need an International Law for information operations", *Lewis & Clark Law Review,* 11(4), 2007, 1023-1061.

- HUGHES, R., "A treaty for cyberspace", *International Affairs,* 86(2), 2010, p. 523-541.

- HUNKER, J.; *et al*., *Role and challenges for sufficient cyber-attack attribution*, Institute for Information Infrastructure Protection, 2008, p. 1-29.

- JENSEN, E. T., "Computer attacks on critical national infrastructure: a use of force invoking the right of self-defence", *Stanford Journal of International Law,* 38, 2002, p. 207-240.

- JENSEN, E. T., "Cyber deterrence", *Emory International Law Review*, 26, 2012, p. 773-825.

- JOYNER, C. C.; LOTRIONTE, C., "Information warfare as international coercion: elements of a legal framework", *EJIL,* 12(5), 2001, p. 825-865.

- KANUCK, S. P., "Information warefare: new challenges for Public International Law", *HILJ,* 37, 1996, p. 272-289.

- KOH, H. H., "International Law in cyberspace", *HILJ Online*, 54, 2012, p. 1-12, available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers, [visited on 22 June 2018].

- KOLB, R., "Reflections on due diligence duties and cyberspace", *GYIL,* 58, 2015, p. 113-128.

- KORZAK, E., "Computer network attcks, self-defence and International Law", in HEHIR, N.; *et al*. (eds.), *International law, security and ethics: policy challenges in the post-9/11 world*, Routledge, 2011, p. 147-163.

- KOSAL, M. E. (ed.), *Technology and the intelligence community: challenges and advances for the 21st Century*, Springer, 2018.

- KURU, H., "Prohibition of use of force and cyber operations as 'force'", *Journal of Learning and Teaching in Digital Age,* 2(2), 2017, p. 46-53.

- LIN, H. S., "Offensive cyber operations and the use of force", *Journal of National Security Law and Policy*, 4, 2010, p. 63-86.

- LIN. H. S., "Escalation dynamics and conflict termination in cyberspace", *Strategic Studies Quarterly*, 6(3), 2012, p. 46-70.

- LEWIS, J. A., *Assessing the risks of cyber terrorism, cyber war and other cyber threats*, Center for Strategic & International Studies, 2002.

- LIBICKI, M. C., *What is information warfare?*, Institute for National Strategic Studies, 1995.

- LYNN, W. J., "Defending a new domain: the Pentagon's cyber strategy", *Foreign Affairs*, 89(5), Sept/Oct 2010, p. 97-108.

- LOMIDZE, I., "Cyber attacks against Georgia", 2011, available at http://www.cert.gov.ge/uploads/GITI%202011/GITI2011_3.pdf,]visited on 22 June 2018[.

- MAHVI, A. J., "Strategic offensive cyber operations: capabilities, limitations, and role of intelligence community, in KOSAL, M. E. (ed.), *Technology and the intelligence community: challenges and advances for the 21st Century*, Springer, 2018, p. 171-182.

- MARGULIES, P., "Sovereignty and cyber attacks: technology's challenge to the law of State responsibility", *Melbourne Journal of International Law*, 14, 2013, p. 496-520.

- MANDEL, R., *Optimizing cyberdeterrence: a comprehensive strategy for preventing foreign cyberattacks*, Georgetown University Press, 2017.

- MAY, L., "The nature of war and the idea of 'cyber war'", in OHLIN, J. D.; *et al.* (eds.), *Cyberwar: law and ethics for virtual conflicts*, OUP, 2015, p. 3-15.

- MELZER, N., *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research (UNIDIR), 2011, p. 1-38.

- MINISTERIO DE DEFENSA, *El ciberespacio. Nuevo escenario de confrontación*, CESEDEN, 2012.

- MOORE, H.; ROBERTS, D., "AP twitter hack cause panic on wall street and sends dow plunging", *The Guardian,* 23 April 2013, available at

https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall, [visited on 15 February 2017].

- MORAN, S., "La ciberseguridad y el uso de las tecnologías de la informacion y la comunicación (TIC) por el terrorismo", *REDI*, 69(2), 2017, p. 195-221.

- MURPHY, J. F., "Cyber war and International Law: does the International Law process constitute a threat to US vital interests?", *International Law Studies*, 89(1), 2013, p. 309-340.

- NAKASHIMA, E.; WAN, W., "China's denials on cyber attacks undercut", *Washington Post,* 25 August, 2011, available at https://www.highbeam.com/doc/1P2-29477839.html,]visited on 22 June 2018[.

- NAVARRETE, I., "L'espionnage en temps de paix en Droit International Public", *CYIL*, 53, 2015, p. 1-65.

- NEY, M.; ZIMMERMANN, A., "Cyber security beyond the military perspective: International Law, 'cyberspace' and the concept of due diligence", *GYIL*, 58, 2015, p. 51-66.

- O'CONNELL, M., E.; *et al*., "Cyber security and International Law", *International Law Meeting Summary, Chatham House*, of 29 May 2012, p. 1-12.

- O'CONNELL, M, E., "Cyber security without cyber war", JCSL*,* 17(2), 2012, p. 187-209.

- OHLIN, J. D.; *et al*. (eds.), *Cyberwar: law and ethics for virtual conflicts*, OUP, 2015.

- PETRAS, C. M., "The use of force in response to cyber-attack on commercial space systems-re-examining self-defence in outer space in light of the convergence of US military and commercial space activities", *Journal of Air Law an Commerce,* 67, 2002, p. 1213-1268.

- REMUS, T., "Cyber-attacks and International Law of armed conflicts; a *jus ad bellum* perspective", *Journal of International Commercial Law and Technology*, 8(3), 2013, p. 179-189.

- REINISCH, A.; BEHAM, M., "Mitigating risks: inter-State due diligence obligations in case of harmful cyber incidents and malicious cyber activity-obligations of the transit State", *GYIL*, 58, 2015, p.101-112.

- ROBLES, M., "El concepto de arma cibernética en el marco internacional: una aproximación functional", *Documento de Opinión 101/2016*, Instituto Español de Estudios Estratégicos, 2016, p. 353-370.

- ROSCINI, M., *Cyber operations and the use of force in International Law,* OUP, 2014.

- ROSCINI, M., "Evidentiary issues in international disputes related to state responsibility for cyber operations", *Texas International Law Journal,* 50(2), 2015, p. 233-273.

- ROSCINI, M., "Digital evidence as a means of proof before the International Court of Justice", *JCSL*, 21(3), 2016, p. 541-554.

- ROSCINI, M., "World wide warfare-*jus ad bellum* and the use of cyber force", *Max Planck UNYB*, 14, 2010, p. 85-130.

- ROSCINI, M., "Cyber operations as a use of force", in TSAGOURIAS, N.; BUCHAN, R. (eds.), *Research handbook on International Law and cyberspace.* Edward Elgar, 2015, p. 233-254.

- RYAN, D. J.; *et al*., "International cyberlaw: a normative approach", *Georgetown Journal of International Law,* 42, 2010-2011, p. 1161-1199.

- RID, TH.; BUCHANAN, B., "Attributing cyber attacks", *The Journal of Strategic Studies*, 38(1-2), 2014, p. 4-37.

- SCHMITT, M. N., "Computer network attack and the use of force in International Law: thoughts on a normative framework", *Columbia Journal of Transnational Law*, 37, 1999, p. 885-926.

- SCHMITT, M. N.; O'DONNELL, B. T. (eds.), *Computer network attack and International Law*, 76, Naval War College, 2002.

- SCHMITT, M. N., "Cyber operations in International Law: the use of force, collective security, self-defense and armed conflicts", in *Proceedings of a Workshop on Deterring CyberAttacks. Informing Strategies and Developing Options for U.S. Policy,* 2010, p. 151-178.

- SCHMITT, M. N., "Cyber operations and the *jus ad bellum* revisited", *Vilanova Law Review,* 56, 2011, p. 569-606.

- SCHMITT, M. N., "International Law in cyberspace: the Koh speech and Tallinn Manual juxtaposed", *HILJ*, 54, 2012, p. 13-37.

- SCHMITT, M. N., "'Attack' as a term of art in International Law: the cyber operations context", *2012 4th International Conference on Cyber Conflict (CYCON 2012),* IEEE, 2012, p. 283-293.

- SCHMITT, M. N., "The law of cyber warfare: *quo vadis*", *Standford Law & Policy Review*, 25, 2014, 269-299.

- SIMONET, L., "L'usage de la force dans le cyberspace et le Droit International", *AFDI*, 58, 2012, p. 117-143.

- SHAKARIAN, P., "Stuxnet: cyberwar revolution in military affairs", *Small War Journal*, 2011, p. 1-10, available at file:///C:/Users/hamed/Downloads/ADA546439%20(3).pdf,]visited on 22 June 2018[.

- SHACKELFORD, S. J., "From nuclear war to net war: analogizing cyber tacks in International Law", *Berkeley Journal of international law*, 27(1), 2009, p. 192-252.

- SHARP, W. G., *Cyberspace and the use of force*, Aegis Research Corporation, 1999.

- SHULMAN, M. R., "Discrimination in the laws of information warfare", *Columbia Journal Transnational Law*, 37, 1999, p. 939- 968.

- SKLEROV, M. J., "Solving the dilemma of State responses to cyber attacks: a justification for the use of active defences against states who neglect their duty to prevent", *Military Law Review,* 201, 2009, p. 1-103.

- STEINER, H., "Cyber operations, legal rules and State practice: authority and control in International Humanitarian Law", Thesis unpublished , *Stockholm University*, 2017.

- TIKK, E., *et al*., *Cyber attacks against Georgia: legal lessons identified*, CCDCOE, November 2008, p. 1-45,at p. 12, available at http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf,]visited on 23 May 2018[.

- TIKK, E.; *et al., International cyber incidents: legal considerations*, NATO Cooperative Cyber Defence Centre of Excellence, 112, 2010, available at https://ccdcoe.org/publications/books/legalconsiderations.pdf, [visited on 2 March 2018].

TODD, G, H., "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition", *Air Force Law Review*, 64, 2009, p. 65-107.

- TSAGOURIAS, N., "Cyber attacks, self-defence and the problem of attribution", *JCSL*, 17(2), 2012, p. 229-244.

- TRINBERG, L., "EU-NATO relations: hand in hand against cyber attacks", 13 January 2017, available at https://ccdcoe.org/eu-nato-relations-hand-hand-against-cyberattacks.html, [visited on 8 June 2018].

- VENTRE, D., *Information warfare,* 2nd ed., Wiley ISTE, 2016.

- WATTS, S., "Combatant status and computer network attack", *VJTL,* 50(2), 2010, p. 391-447.

- WALTER, Ch., "Obligations of States before, during, and after a cyber security incident", *GYIL*, 58, 2015, p. 67-86.

- WAXMAN, M. C., Cyber-attacks and the use of force: back to the future of article 2(4), *YJIL*, 36(2), 2011, p. 421-459.

- WAXMAN, M. C., "Cyber attacks as 'force' under UN Charter article 2 (4)", *International Law Studies,* 87(1), 2011, p. 43-57.

- WAXMAN, M. C., "Self-defensive force against cyber attacks: legal, strategic and political dimensions", *International Law Studies*, 89, 2013, p. 109-122.

- WHEELER, D. A.; *et al*., *Techniques for cyber attack attribution*, Institute for Defence Analyses, No. IDA-P-3792, October 2003.

- WINGFIELD, Th., *When is a cyber attack an 'armed attack'?: legal thresholds for distinguishing military activities in cyberspace*, Cyber Conflict Studied Association, 2006.

- ZIOLKOWSKI, K. (ed.), *Peacetime regime for State activities in cyberspace*, NATO CCDCOE, 2013.