THE CHALLENGES OF ATTRIBUTION OF INTERNATIONALLY WRONGFUL ACTS IN THE CYBERSPACE: A CRITICAL ANALYSIS OF CONTROL TESTS AND THE STANDARD OF PROOF IN INTERNATIONAL COURTS

Os desafios da atribuição de atos ilícitos internacionais no espaço cibernético: uma análise crítica dos testes de controle e do nível de prova nas cortes internacionais

Filipe Gomes Dias Costa[*]
Verônica Lúcia Hassler Benn[**]

RESUMO: Este artigo discute os aspectos legais, os desafios e dificuldades que as teorias tradicionais do direiro internacional enfrentam quando se trata da atribuição de responsabilidade no mundo cibernético. Primeiro, será explicado como o espaço cibernético é visto do ponto de vista do direito internacional. Em seguida será feita uma análise sobre os níveis de prova e os testes de atribuição e como eles funcionam em situações tradicionais. Após, será realizada uma abordagem crítica sobre a ineficiência dessas regras quando aplicadas nas condutas dos Estados no mundo cibernético. Finalmente, será analisado o principio do *"due diligence"* e a mitigação do nível de prova como possíveis soluções para este dilema, em conjunto com a necessidade da codificação e da adaptação dos testes de atribuição para se adequarem às particularidades do espaço cibernético.

PALAVRAS-CHAVE: Responsabilidade dos Estados. Direito Cibernético. Atribuição. Testes de Controle. Nível de prova.

* Graduando em Direito pela Universidade Federal da Bahia. Membro-fundador do Núcleo de Competições Internacionais da Faculdade de Direito da Universidade Federal da Bahia (NCI – FDUFBA). E-Mail: filipe_costa40@hotmail.com
** Graduanda em Direito pela Universidade Federal da Bahia. Membro do Núcleo de Competições Internacionais da Faculdade de Direito da Universidade Federal da Bahia (NCI – FDUFBA). E-Mail: veronicahasslerb@gmail.com

THE CHALLENGES OF ATTRIBUTION OF INTERNATIONALLY WRONGFUL ACTS IN THE CYBERSPACE

ABSTRACT: This paper discusses the legal aspects, the challenges and difficulties that the traditional theories face when dealing with attribution on the cyber world. First, it will explain how the cyberspace is seen on the international law context. Following, it will be made a close examination of the standard of proof and the attribution tests, and how they work on regular situations. Then, it will be made a critical approach on the inefficiency of this rules when applied on State conducts on the cyberspace. Finally, the due diligence principle and the mitigation of the standard of proof will be analyzed as proper solutions to this dilemma, along with the need for proper codification and adaptation of the control tests to the particularities of the cyberspace.

KEYWORDS: State Responsibility. Cyber law. Attribution. Control Tests. Standard of Proof.

1 INTRODUCTION

The law of State responsibility is one of the most important subjects in international law. The codification of the Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)

is one of the cornerstones of the development of international law and represent not only codification of customary law, but also a progressive development on the field of State responsibility.

However, not all situations can be simply resolved by easily applying the rules of the ARSIWA. There are often cases in which there are difficulties in the attribution of a wrongful act to a State.

The development of new technologies in the second half of the 20th century has led to the creation of a whole new place for international relations to be held, commonly referenced as cyberspace.

With such innovations, it is necessary for the international law to accordingly evolve in order to regulate possible violations committed by international subjects. In this regard, the norms of attribution constitute one of its most severed fields due to their incompatibility with the particularities of the cyberspace.

Hence, it is necessary to rethink the norms surrounding the attribution of internationally wrongful acts, especially the attribution tests used by international courts and the commonly applied standard of proof.

2 INTERNATIONAL LAW ON THE CYBERSPACE

Cyberspace may be understood as a global, non-physical, conceptual space, which includes physical and technical components, the internet, the 'global public memory' contained on publicly accessible websites, as well as all entities and individuals connected to the internet (ZIOLKOWSKI, 2013, p. 135). In the actual word, the cyberspace goes far beyond the notion of a pure means of information transfer, having political, economic, social and cultural aspects.

Even though such position is now regarded as outdated, there are scholars who still defend that cyberspace is not, or is only partly, regulated by law, since cyber-specific international custom is absent and contractual regulations are scarce. The classical international law consequence to such situation would be to invoke the basic principle stated in 1927 by the Permanent Court of International Justice (PCIJ) in the Lotus case (GLENNON, 2002). Such principle establishes that, in the absence of a legal prohibition, a State enjoys freedom of action (DEEKS, 2015, p. 301). In the cyber context, this line of thought emanates primarily from the notion that the cyberspace would constitute a whole new international domain that would require special regulations, such as the Law of the Sea or the Law on Outer Space.

Nonetheless, such concept is minority among the international community, since the existence of *non liquet* would lead to serious consequences in the international relations of States, which are now, more than ever, undertaken through cyber assets.

Furthermore, the idea of cyberspace as a separate and independent domain would ultimately contradict the very mechanisms from which the cyberspace is built upon (CZOSSECK, 2013, p. 15). As stated before, cyberspace is nothing more than the collection of physical assets that collectively sustains the shapeless cloud regarded as cyberspace. Servers, backbones, and even fiber optic cables are all pillars of this amalgam and, undoubtedly, are subject to the regulations of law.

Therefore, one may not argue that the cyberspace is absent from the incidence of international law whatsoever, since, although it is not yet possible to extract customary norms from state practice, the general principles of international law as they exist are indeed applicable to this niche of international law.

In this respect, the consequently competing freedoms of the coexisting sovereign States are guided by general principles of international law. These principles are most important in the cyber context, since they form the basis for a progressive development of international law, enabling the international law system to respond to the dynamic needs of an international society and especially to meet the growing technological advances (ZIOLKOWSKI, 2013, p. 135). Accordingly, the general principles of international law occupies the position of cornerstones from which the law on the cyberspace would be developed.

Consequently, although the law on cyberspace is not yet consolidated, it may not be regarded as a wild west in which there are no application of basic norms. However, such field of international law shall be urgently one of the primary focus of scholars and States in regard to the development of International law, since the mere application of basic principles of law may lead to misconceptions and failures to satisfactorily respond to a given situation.

Such problem is found in the matters regarding the attribution of cyber attacks under international law, especially due to its traditional approach and, therefore, irreconcilable with the new mechanisms developed in the cyberspace.

3 THE NECESSARY CONDITIONS FOR A STATE TO BE HELD RESPONSIBLE FOR AN INTERNATIONAL WRONGFUL ACT

3.1 Attribution on international law

The rules of attribution of responsibility were codified on the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). In the ARSIWA, it is established that a State will be

deemed responsible for the acts of its organs, regardless of their composition and function. Thus, the acts of the executive, legislative, judiciary and armed forces would be attributed to the State they belong.

As a general principle, the conduct of private persons or entities is not attributable to a State under international law. However, there are circumstances where such conduct is nevertheless attributable because a specific factual link exists between the person or entity engaging in the conduct and the State.

The Draft Articles in its article 8 establishes that:

> Article 8. Conduct directed or controlled by a State
>
> 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, that State in carrying out the conduct.

It is clear then that a State may, either by specific directions or by exercising control over a group, assume responsibility for their conduct. Each case will depend on its own facts, in particular those concerning the relationship between the instructions given, the direction or control exercised. In the text of article 8, the three terms "instructions", "direction" and "control" are disjunctive; it is sufficient to establish any one of them. At the same time it is made clear that the instructions, direction or control must relate to the conduct which is said to have amounted to an internationally wrongful act.

Thus, article 8 brings two situations. The first involves private persons acting on the instructions of the State in carrying out the wrongful conduct. The second deals with a more general situation where those private entities or persons act under the State's direction or control. Bearing in mind the important role played by the principle

of effectiveness in international law, it is necessary to take into account in both cases the existence of a real link between the person or group performing the act and the State machinery.

This link is essential to the matter of attribution, since the conduct will only be attributable to the State 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.

The degree of control which must be exercised by the State in order for the conduct to be attributable is a key issue in international law. Currently there are two attribution tests used by the Courts. The first is the effective control test, created by the International Court of Justice (ICJ), and the second is the overall control test, originated from the International Criminal Tribunal for the Former Yugoslavia (ICTY).

3.1.1 Effective control

In the *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* the ICJ had to decide if the human rights violations committed by the *Contras*, a rebel group fighting the Nicaraguan army on the civil war, could be attributed to the United States, since they had received help from the US during the war.

The Court identified three forms of "private" conduct that could generate state responsibility: the paramilitary campaign in general, specific military operations and the humanitarian law violations committed by the *Contras* in the course of operations. Regarding the specific missions of the *Contras*, the State of Nicaragua was unable to establish a real bond between the United States and one

of these operations, and could only argue the American involvement in the movement in general.

In its decision the Court considered that, although the United States had not created the *Contras*, he was responsible for financing, giving logistical support and military training to the group. However, the ICJ ruled that the United States could not be held responsible for the general activities of the *Contras*. The Court based its decision on the fact that the US exercised insufficient control over the *Contras*, which were not completely dependent on the US in a way that any act done by them would give rise to liability.

For the ICJ, even all the forms of participation and even the general control by the US over the group, which had a high degree of dependency on the State, would not in themselves mean, that the US directed or enforced the perpetration of the acts contrary to human rights and humanitarian law and such acts could be committed by members of the *Contras* without the control of the United States. For this conduct to give rise to legal responsibility of the United States, 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.

On the Bosnian Genocide case the ICJ identified this sense of complete dependence with the term *"de facto organ"* in the context of ARSIWA article 4. This kind of organ, even though is not considered a State organ, like the judiciary or the military, is completely linked to the State, not having autonomy and being completely dependent.

The Court, nevertheless, considered that there was a violation of the prohibition of the use of force, based on the direct support given to the paramilitary group.

Hence, for the effective control test, the mere support to a group or private entity does not creates responsibility, unless the State has full control over the actions of these entities at the time of the act.

3.1.2 Overall Control

In contrast to the effective control test, the International Criminal Tribunal for the Former Yugoslavia, on the *Tadic case*, established the overall control test. Dusko Tadic was in trial on the ICTY for crimes against humanity, serious breaches of the Geneva Conventions, and violations of customs of war by the for his actions in the Prijedor region, including the Omarska, Trnopolje and Keraterm detention camps[1].

Since the ICTY is a tribunal with jurisdiction limited to individuals, it is not usually considered able to deal with questions of State responsibility. In the *Tadic* case, however, the Tribunal had to analyze State responsibility as a preliminary question, in order to determine whether the armed conflict was international or not, and, therefore, whether the Court had jurisdiction over it[2]

In order to define if the war was or not an international conflict, the ICTY chamber pondered the relationship between the three ethnic groups in the region (Orthodox Christian Serbs, Croats Roman Catholics and Bosnian Muslims) and the external influence of the States involved. If these states were considered responsible for the activities of private entities operating in Bosnia, the conflict would be considered international. The Court focused especially on the acts of the Republic of Srpska one of the autonomous entities of Bosnia and

[1] The Bosnian War was an international armed conflict that took place in Bosnia and Herzegovina between 1992 and 1995. The main belligerents were the forces of the Republic of Bosnia and Herzegovina and those of the self-proclaimed Bosnian Serb and Bosnian Croat entities within Bosnia and Herzegovina, Republika Srpska and Herzeg-Bosnia, who were led and supplied by Serbia and Croatia respectively.

[2] That was relevant once the Genebra Convention of 1945 is only applicable to international conflicts.

Herzegovina, which was contrary to the independence and whose army was responsible for the Srebrenica massacre, in which 8,373 Bosnian Muslims were killed.

The vast majority of the judges used the *Nicaragua case* in order to determine whether the Republic of Yugoslavia could be held responsible for the acts of the Republic Srpska, but without distinguishing clearly between the full and effective control tests established by the ICJ. The Court held that the Srpska Republic, although an ally of Yugoslavia and dependent of their assistance, could not be considered under its control.

The Appeals Chamber reviewed the case in 1999. The Chamber reaffirmed the decision to use State responsibility rules to determine the international dimension of the conflict, but at the same time, criticized the use of the *Nicaragua case* as an attribution standard. For the Appeals Chamber, the notion of effective control was contrary to the "logic" of the responsibility of States, since it allowed the States to use private entities to commit acts that could not be performed by its own organs, managing to escape international responsibility.

The Chamber stressed that the requirement of international law for the attribution to States of acts performed by private individuals is that the State exercises control over the individuals. The degree of control may, however, vary according to the factual circumstances of each case. The Appeals Chamber did not see why in each and every circumstance international law should require a high threshold for the test of control.

In this regard, the Chamber created a distinction between the level of control necessary in relation to unorganized groups and structured organized groups. If the group or individuals in question are not organized, an effective control over the specific acts can generate responsibility, while in organized groups only general control would

suffice. Therefore, in the case of organized groups, if the state has a role in organizing, financing or planning the actions of these groups it may create international responsibility. The Tribunal accepted this view and has consistently applied in its decisions[3].

Thus, the Chamber held that the degree of control by the Yugoslav authorities over the armed forces, required by international law for considering the armed conflict to be international, was overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations.

In the course of their reasoning, the majority considered it necessary to disapprove the ICJ approach in the *Military and Paramilitary Activities in and against Nicaragua case*. However the legal issues and the factual situation in the *Tadic case* were different from those facing the Court in that case. The Tribunal's decision is directed to issues of individual criminal responsibility, not State responsibility, and the question in that case concerned not responsibility but the applicable rules of international humanitarian law.[4]

The overall control test is still criticized in international law, including by the own ICJ. In the *Bosnian Genocide case*, which was generated from the same conflict of the *Tadic case*, the Court was called upon to examine whether Yugoslavia (and later Servia) was responsible for the genocide committed by the militia during the Bosnian War.

[3] For example: Prosecutor v. Alekovski, Prosecutor v. Kordic e Prosecutor v. Naletilic

[4] The problem of the degree of State control necessary for the purposes of attribution of conduct to the State has also been dealt with, for example, by the Iran-United States Claims Tribunal and the European Court of Human Rights: Yeager (see footnote 101 above), p. 103. See also Starrett Housing Corporation v. Government of the Islamic Republic of Iran, Iran-U.S. C.T.R., vol. 4, p. 122, at p. 143 (1983); Loizidou v. Turkey, Merits, Eur. Court H.R., Reports, 1996–VI, p. 2216, at pp. 2235–2236, para. 56, also p. 2234, para. 52; and ibid., Preliminary Objections, Eur. Court H.R., Series A, No. 310, p. 23, para. 62 (1995)

The ICJ considered that, even in the case a serious crime as genocide, there was no justification for not making use of the effective control test. In its decision the Court criticized the stance of the ICTY, arguing that despite the Tribunal being an authority on international criminal law, it would not have the ability to express opinions outside its jurisdiction. The Court, dealing specifically with the overall control test, established that it was improper to be applied in the attribution of state responsibility, since it did not align with the primary rules of international law and the secondary rules of State responsibility.

Regardless of this, both tests are still used, and are considered to be the basic standard regarding the attribution of private acts to a State.

3.2 Evidence of State involvement

In order for a State to be held responsible for an international wrongful act, it must exist sufficient evidence of its involvement on the acts considered wrongful. Therefore, under international litigations, the procedural stage of evidence analysis is as important as the definition of the attribution test applicable to a given case.

Although the matters concerning the burden of proof is well settled in international litigations, the standard of proof applicable configures one of the most crucial and defining questions to a judicial case in international law.

In regard to cyber attacks, this importance is further enhanced, since the usage of classical standards of proof may lead to the failure altogether of a plaintiff's attempt of attribution to a State.

It is established that, while in civil law systems there are no specific standards of proof that judges must apply, common law jurisdictions employ a rigid classification of standards. From the most to the least stringent, these include: beyond reasonable doubt (i.e.,

indisputable evidence, a standard used in criminal trials), clear and convincing (or compelling) evidence (i.e., more than probable but short of indisputable), and the preponderance of evidence or balance of probabilities (i.e., more likely than not or reasonably probable, a standard normally used in civil proceedings). A fourth standard is that of prima facie evidence, a standard that merely requires indicative proof of the correctness of the contention made (ROSCINI, 2015, p. 248).

Even though the International Court of Justice in its Statute and Rules of the Court does not indicate specific standards of proof for particular cases, the Court has adopted the practice of referring to expected standards in the judgments itself. In this sense, the Court has adopted a mixed concept, in which, in line with civil law practice, it may choose case by case the suitable degree of evidence, but must also indicate the specific standard adopted under the predetermined criteria established by common law systems.

Nonetheless, it is possible to extract from the jurisprudence of the Court, established practice regarding the definition of standard of proof in order to accurately predict the standard adopted in certain matters of International Law. This is the case of allegations of use of force, in which at least clear and convincing evidence is expected for such claims, demonstrating that the Court does apply standards in accordance with the nature of the allegations.[5]

[5] See Nicaragua case, Oil Platforms case and Dem. Rep. Congo v. Uganda.

4 THE HARDSHIPS OF ATTRIBUTION IN THE CYBER CONTEXT

4.1 Attribution and the Tallinn Manual

Between 2009 and 2012, an international group of approximately twenty experts were convened by the NATO Cooperative Cyber Defense Centre of Excellence to work on a draft for a manual addressing the issue of how to interpret international law in the context of cyber operations and cyber warfare. Of their work it was created the *Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual)*

The *Tallinn Manual* is an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare. As such, it was the first effort to analyse this topic comprehensively and authoritatively and to bring some degree of clarity to the associated complex legal issues (SCHMITT, 2013). The Manual contemplates and examines 'how extant legal norms applied to this "new" form of warfare' (Introduction, p 1) thus pursuing the purpose of 'bringing some degree of clarity to the complex legal issues surrounding cyber operations' (p 3). While the term 'cyber warfare' is used in a 'purely descriptive, non-normative sense' (p 4, n 17), the main focus of the Manual is armed conflict proper, i.e. armed 'hostilities, which may include or be limited to cyber operations' (pp 7 - 9 Rules 22 and 23). However the Manual is not designed for addressing what may be considered as the predominant issue, how to ensure cyber security against criminal activities by hackers (O' CONNELL, p. 203, 2013).

Following the principle established in the *Corfu Channel case*, the Manual on its Rule 5 established that a State "shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States". The Experts agreed that

this Rule covers all acts that are unlawful and that have detrimental effects on another State.

Yet, they could not agree whether that Rule applies only to cyber operations that are underway or also in situations in which those acts are 'merely prospective' (para 7); whether it applies only to actual knowledge or also to 'constructive ("should have known") knowledge' (para 11); and whether it only applies to cyber activities on a state's territory or also to states through which these cyber operations are routed (para 12). On the Rule 6, the Experts acknowledged that conduct of non-state actors may be attributable to a State.

On the matter of attribution, the *Manual* largely imports this restrictive language from the International Law Comission and the case law. It cites both the 'effective' and 'overall' control tests (SCHMITT, 2013, p. 46). Tellingly, it does not cite the language from *Tadić* which describes general helping behavior as meeting the overall control test. Instead, the *Manual*'s drafters included other language that was more rigid, in which it opined that a finding of state responsibility required official participation in the planning and supervision of military operations. On this view, a state would not share responsibility under international criminal law for harm a private group causes in cyber activities unless the state did more than finance and equip the group.

4.2 The problem of the standard of proof and control test on the cyber world

The question arises whether there is a need for special, and lower, standard in the cyber context. Despite, the lack of case law in the ICJ in relation to claims arising out of inter-state cyber operations, possible indications regarding the standard of proof may be found elsewhere. The Project Grey Goose Report on the 2008 cyber operations against Georgia, for instance, relies on the concordance of

various pieces of circumstantial evidence to suggest that the Russian government was responsible for the operations. Such standard, although already applied by the ICJ in the *Corfu Channel* case, has been widely regarded as an insufficient mechanism to prove the existence of an internationally wrongful act. In this sense, the Court has stated in the same judgment that such standard may only be used in exceptional allegations, which does not include attribution itself.

Notwithstanding, the particularities of cyberspace itself create inherent obstacles to satisfy the traditional standard of proof applied by international courts. As the Tallinn Manual states, there are several ways in which the possibility of attribution may be hindered. IP routing, spoofing and others vicarious benders nullify the classical rules of attribution due to their ability to derail any proof regarding the link between a cyber attack and its perpetrator. This dilemma may lead to the impunity of such breaches of international law and constitute a serious liability of contemporary International Law.

On the same note, the attributions tests adopted by the International Courts may lead to impunity for States who engage on cyber activities since both tests require a high level of control, which is hard to proof on the cyber context.

The effective control and the overall control establish that it must be proved that a State had a certain level of control over the individuals and entities. For the effective control, this control must be in a way that the group shows no autonomy, being completely dependent of the State. This kind of control is hard to proof on the "real" word, but on the cyber context is almost impossible, since, the hackers' activities hardly ever could be traced.

Even though when a cyber attack is launched from its governmental cyber-infrastructure it is considered as an indication that a State is associated with the attack (SCHMITT, 2013, p. 39), and the method of comparison of code fragments used in malicious software

can also indicate the provenance (Pihelgas, 2013, p. 38), this is not enough evidence to invoke attribution.

As the *Tallinn Manual* states, the usage of cyber governmental structures does not constitute enough evidence to attribute the operation to that State. It is considered that, on cyber structures, it is more likely that government infrastructure could have been taken over by non-state actors without State authorization (SCHMITT, 2013, p. 35). This is due to the impossibility to conclude if a cyber attack originated from the place where the IP is traced.

Furthermore, the identification of similarity between softwares only provides a probability of authorship rather than a certainty, and this does not prove attribution, since third party could buy, steal or gain access to another's malware (ROWE, 2015).

Hence even when it is discovered that the cyber activity originated from the cyber infrastructure of a State organ or that the malware used was created by the State, for the effective control approach, there would not be enough evidence of control and dependence.

At first it may appear that the overall control test, which lowers the standard of attribution, would be the solution to the problem of attribution on the cyber realm. However this test is also insufficient on the cyber context, since, as mentioned above, it would also require proof of not only a general control, but also the knowledge of it the group is organized or not in order for the standard to be lowered.

Thus, considering that conclusive evidence against a State on the cyber realm is difficult to collect, to this day, States have great freedom to engage on cyber activities even when the acts committed constitute an international wrongful act. This was shown by the

Stuxnet malware[6] and Titan Rain incidents[7], in which no State was deemed responsible, giving the difficulties to properly invoke international responsibility. Therefore, cyber incidents are highly incompatible with the current tests of attribution.

5 POSSIBLE SOLUTIONS

5.1 Due diligence

The duty of due diligence is a well-established principle in international law. According to this principle, States must use due diligence to prevent the commitment, within its jurisdiction, of illicit acts against another State or its people. This obligation comprises any actions that produce detrimental effects on another State, including criminal activities conducted by private actors.

As the *Tallinn Manual* itself establishes, it is still unclear whether a State violates its duty if it fails to use due care in policing cyber activities on its territory and is therefore unaware of the acts in question due to the difficulty of attribution and the easiness in which cyber attacks can be mounted through others cyber infrastructure. Furthermore, some scholars have suggested that no duty of prevention exists in the cyber context given the difficulty of mounting comprehensive and effective defenses against all possible threats. It is

[6] Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon.Although neither state has confirmed this openly, anonymous US officials speaking to the Washington Post claimed the worm was developed during the Obama administration to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.

[7] Titan Rain was the designation given by the federal government of the United States to a series of coordinated attacks on American computer systems since 2003. In early December 2005 the director of the SANS Institute, a security institute in the United States, said that the attacks were "most likely the result of Chinese military hackers attempting to gather information on U.S. systems.

thus, not yet established whether a State violates international law if it fails to apply due diligence in policing cyber activities on its territory.

However, it is also understand that States shall not allow its cyber infrastructure to be used for committing acts that unlawfully affect other States. Where a potentially problematic activity has been launched from cyber infrastructure which is exclusively used by the government of a State, a rebuttable presumption can apply that the State should have known of this use of its territory (HEINEGG, 2012, p. 17).

Also, scholars have stated that States have an obligation to prevent private actors from freely using (SCHMITT, 2015, p. 72) its governmental computer infrastructure or freely transiting through it (BANNELIER-CHRISTAKIS, 2014, p. 8) even if an attack is originated from outside of its territory.

Due diligence principle also includes taking precautionary measures at an early stage before the concrete risk of harm occurs. This Court held that due diligence implies the exercise of administrative control. Monitoring activities and taking precautionary measures on cyber-infrastructure are therefore representative of the due diligence principle in the cyber context (ZIOLKOWSKI, 2013, p. 167).

This principle also covers the duty to investigate and punish non-State actors that have committed crimes against other States (ARÉCHAGA 1968, p. 531; AGO, 1970), and the General Assembly has called upon States to prevent criminal misuse of information[8].

Hence, the due diligence principle should be applicable to the cyber context, once the attribution tests are inadequate when applied

[8] GA Resolution A/RES/55/63, pg 2 (a); GA Resolution A/RES/56/121; GA Note by the Secretary-General A/68/98, pg 8, para 23.

to the cyber realm. By using this principle, it would be possible for a State to be held responsible even if it the act itself cannot be attributable to this State. Since the violation of the due diligence obligation must be assessed based on State's' level of development and technical capabilities, more development States could not excuse themselves for their inability to prevent, or to take any action against breaches of international law that occur on their cyber space

Therefore, the application of the due diligence principle could be a possible solution to the situation regarding the responsibility of States on the cyber world, as it may bring State responsibility for any cyber act that can be considered wrongful, or at least, for its fail to prevent such act to happen.

5.2 Mitigation of the standard of proof

The Statute of the International Court of Justice states in its Article 48 that:

> Article 48
>
> The Court shall make orders for the conduct of the case, shall decide the form and time in which each party must conclude its arguments, and make all arrangements connected with the taking of evidence.

Such norm illustrates the freedom that the ICJ enjoys in regard to evaluate evidence itself. In previous cases, the Court has already lowered the expected standard of proof to resonate with the allegations in discussion (VALENCIA-OSPINA, 1999, p. 203). Thereafter, such mitigation has only been applied using the nature of the allegations as the modulator. However, such adaptation may not be restricted to the allegations raised by the parties. Foremost, the purpose of evidence itself is to prove the existence of a given fact. Consequently, the Court is allowed to ease its standard of proof to

adequate it to the nature of certain facts. Such conclusion is extracted directly from the Statute of the Court itself, and is it is in line with the majority doctrine, which argues that the ICJ enjoys the right to define its rules regarding evidence in accordance with the particularities of the cases.

In regard to the question surrounding attribution of cyber attacks, due to the unviability to properly attribute a cyber incident to an international actor, it is indispensable to lower the standard of proof, even if facing allegations of use of force. This is due to the fact that the viability of a proper judgment, the due process of law and fair trial would be at stake, since the possibility to attribute an internationally wrongful act of a cyber nature would be virtually impossible due to evidentiary problems.

Therefore, the mitigation of the standard of proof may configure as one of the most necessary mechanisms in order to adapt the litigation under international to the particularities of the cyberspace. In this sense, the notion of circumstantial evidence appears as the most suitable standard to settle cyber attacks matters, with no prejudice to the creation of a new degree of evidence.

6 CONCLUSIONS

Due to the progressively outdating of the norms of attribution in face with the cyber context, especially in regard to cyber attacks, it is necessary the establishment of revised norms of attribution to adequate the cyberspace with the normative incidence of International Law.

In this line, the Tallinn Manual configures as an important point of start for the codification of the norms in the cyberspace. However, even though such document does represent a relevant

collection of guidelines, its dispositions regarding attribution of cyber incidents lacks concrete innovations. The heavy influence from the Articles on Responsibility of States for Internationally Wrongful Acts, although important to settle the basic norms of attribution, may lead to the perpetuation of the present problems involving attribution on the cyberspace. Therefore, it is already needed to revise the Tallinn Manual in order to adequate its norms with the necessity of the new age, albeit it is indeed the most accurate document relating to cyber operations, especially due to its approach of due diligence.

Furthermore, in international litigations, the adequation of the institutes of the control tests and standard of proof is needed to the particularities of the cyber space. Hence, it is necessary to adapt the control tests in order to enable attribution in the cyber context. On the other hand, additionally, the adoption of a lower standard of proof such as the circumstantial evidence may also be a crucial and needed step in order to enable attribution of cyber incidents.

The lack of conformity with the scientific progress is normal to any area of Law. Such outdating is no different with international law, which must constantly evolve and adapt to the new caveat of the contemporary international society. Conclusively, it is flagrant the necessity for international law to adapt to the new paradigms created by the development of technology, at the risk of generating anomy and impunity.

7 BIBLIOGRAPHY

AGO Robert, **Second Report on State Responsibility: The Origin of International Responsibility**, U.N. Doc. A/CN.4/233, (1970)

ARÉCHAGA Eduardo Jiménez de, **Manual of Public International Law,** Edited by: Max Sorensen (1968)

BANNELIER-CHRISTAKIS Karine, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' **Baltic Yearbook of International Law** 14th edn, Brill 2014.

CRAWFORD James R. **Browlie's Principles of Public International Law** 8ª edn, Oxford, ed.Oxford University Press (2012).

CRAWFORD James R**. State Responsibility, the General Part**, 1ª edn, Cambridge ed. Cambridge (2014).

CZOSSECK Christian, **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy: State Actors and their Proxies in Cyberspace**. Edited by: Katharina Ziolkowski, (NATO CCDCOE, 2013).

DEEKS Ashley, An International Legal Framework for Surveillance, **Virginia Journal of International Law**, Charlottesville, Virginia,USA Vol. 55:2 p. 301 (2015).

FLECK, Dieter. Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual, **Journal of Conflict & Security Law** Oxford, ed. Oxford University Press 2013

GLENNON, Michael J., The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter, **Harvard Journal of International Law,** Cambridge, Massachusetts (US) V.49 p. 539 - 555 (2002)

HEINEGG, Heintschel von. **'Legal Implications of Territorial Sovereignty in Cyberspace'** In: 4th International Conference on Cyber Conflict (2012)

INTERNATIONAL COURT OF JUSTICE .*Corfu Channel (UK v Albania)*, Judgment. In: ICJ Reports 4, 22. (1949) The Hague, Netherlands

_____. *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 The Hague, Netherlands

_____. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* Merits, Judgment, In: ICJ Reports 1986. The Hague, Netherlands

_____. ICJ Report 2007 The Hague, Netherlands

_____. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment of 20 April 2010. In: ICJ Reports 2010. The Hague, Netherlands

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. *Prosecutor v. Duško Tadic*, ICTY Case No. IT-94-1-T, Trial Chamber, 7 May 1997, The Hague, Netherlands

_____. *Prosecutor v. Duško Tadic*, Appeal against Conviction (1999) 124 ILR 61, 98-121 The Hague, Netherlands

INTERNATIONAL LAW ASSOCIATION. **International Law Association Study Group on Due Diligence in International Law, 'First Report'** (2014) <https://perma.cc/WX88-SBDX> accessed in 19 December 2015

INTERNATIONAL LAW COMISSION. **Draft articles on Responsibility of States for Internationally Wrongful Acts.** Geneva, 2001

_____. **Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries**, Geneva 2001

MAZZUOLI Valério de Oliveira. **Curso de Direito Internacional Público**, 7ª edn, São Paulo, ed. Revista dos Tribunais 2013

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge,** England, United Kingdom ed. Cambridge University Press (2013)

O'CONNELL, 'Cyber Security without Cyber War' **Georgetown Journal of International Affairs** 17 JCSL 187 (2012)

ONU. General Assembly Resolution A/RES/55/63,

_____. General Assembly Resolution A/RES/56/121;

_____. General Assembly A/68/98.

OPPENHEIM Lassa Francis Lawrence, **Oppenheim's International Law: Volume 1 Peace** (9th edition) Edited By: Sir Robert Jennings QC, Sir Arthur Watts KCMG QC 2008 ed Oxford

PERMANENT COURT OF INTERNATIONAL JUSTICE, *S.S.Lotus (France v.Turkey.*), Merits (1927) In: PCIJ Rep Ser A, No 7, 18ff. The Hague, Netherlands

PIHELGAS Mauno, **Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy: 'Back-Tracing and Anonymity in Cyberspace'**, Edited by: Katharina Ziolkowski (NATO CCDCOE, 2013)

ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. **Texas International Law Journal,** Austin, Texas, US vol. 50, Issue 2 (2015)

ROWE Neil C. '**Attribution of Cyber Warfare' in Cyber Warfare: A Multidisciplinary Analysis**, ed. J. Green, Routledge, http://faculty.nps.edu/ncrowe/3%20-%20Rowe%20chapter%20070214.htm Acessado em: 12 de maio de 2016

SCHMITT Michael, 'In Defense of Due Diligence in Cyberspace' **The Yale Law Journal**, New Haven, Connecticut, U.S. v. 68 (2015)

SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare.** New York, United States of America: Cambridge University Press. (2013)

SHAW Malcolm N. **International Law** 5th Edition, Cambridge, ed. Cambridge University Press (2003)

VALENCIA-OSPINA. Eduardo, '**Evidence before International Court of Justice'** Int'l L.F. D. Int'l (1999)

ZIOLKOWSKI, Katharina. **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publication, Tallinn 2013

Recebido em 15 de maio de 2016
Aprovado em 16 de agosto de 2016