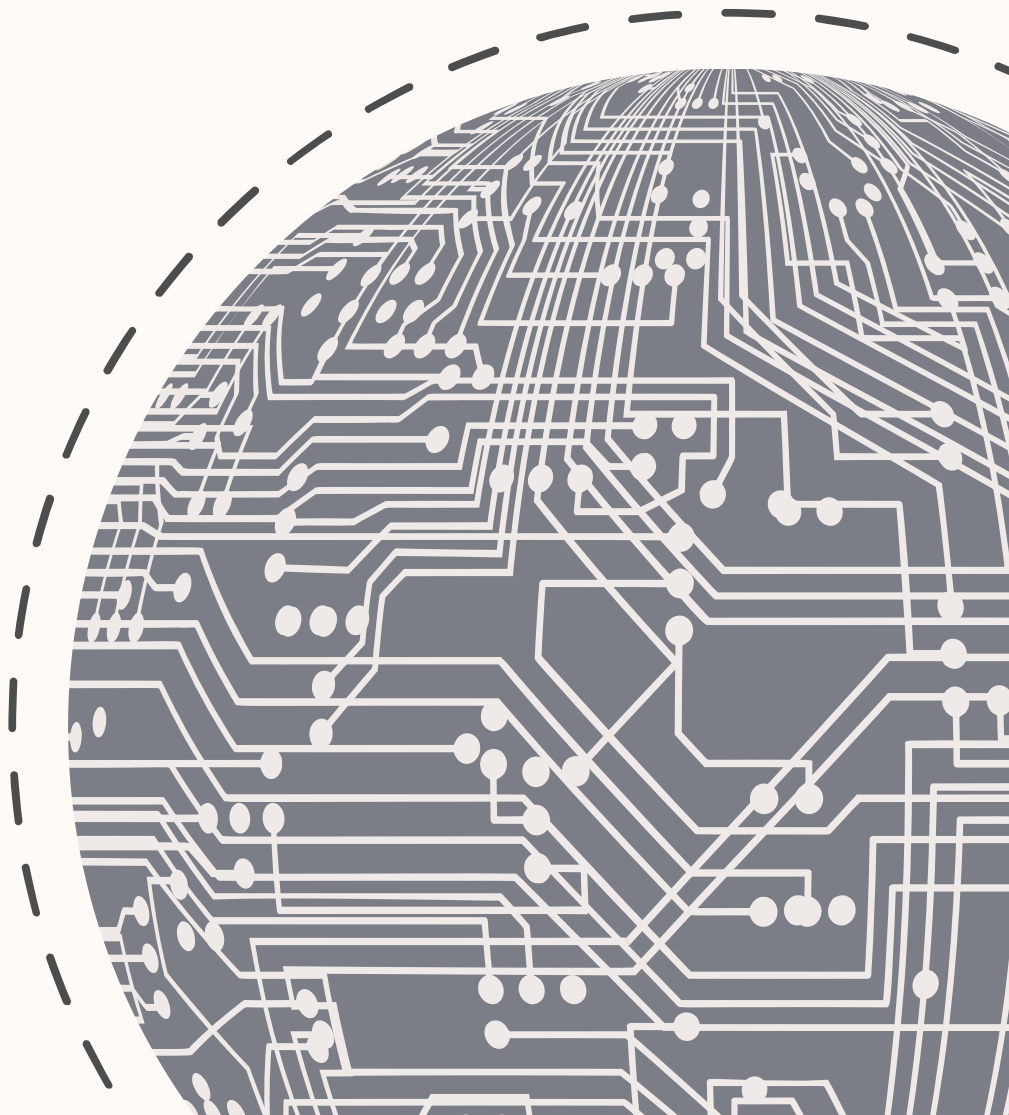
Cancillería

Colombia's National Position on the

APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE

2025



Cancillería

Laura Camila Sarabia Torres
Minister of Foreign Affairs

Mauricio Jaramillo Jassir
Vice Minister of Multilateral Affairs

Andrea Jiménez Herrera
Director of International Legal Affairs

Jhon Jairo Camargo Motta
Director of Multilateral Political Affairs

Rosario Gutiérrez Bernal
Coordinator of Advisory for International Legal Affairs

Laura Quintero Buriticá
Coordinator of Crime Prevention

Álvaro Frías Galván
Third Secretary, Advisory for International Legal Affairs

Lucía Solano Ramírez
Counselor – Legal Advisor, Permanent Mission of Colombia to the UN in New York

Nathalia Trujillo Castro
Intern

Cancillería

TABLE OF CONTENTS

Cancillería

1. Introduction

The application of International Law to the use of information and communications technologies by States has been discussed in the United Nations, within the framework of the then Groups of Governmental Experts (GGE), the Previous Open-Ended Working Group on Security and in the use of Information and Communication Technologies (OEWG 2019-2021), and currently, in the Open-Ended Working Group on Security and in the use of Information and Communication Technologies (2021-2025) (OEWG), established pursuant to resolution 75-240 of the General Assembly.

As the OEWG's Annual Progress Reports have noted, its sessions have been held in a difficult geopolitical environment, with rising concerns over the malicious use of information and communication technologies (ICTs) by State and Non-State actors, targeting critical infrastructure and essential services. In this scenario, States, including Colombia, have recalled and affirmed that International Law, in particular the Charter of the United Nations, is applicable to cyberspace and is essential to maintain peace, security and stability and to promote an open, secure, stable, accessible and peaceful ICTs environment.

In this context, Colombia's position on this issue is set out below with the purpose of contributing to advancing a robust and inclusive framework for the application of International Law in the use of ICTs, avoiding misunderstandings, increasing predictability and stability in cyberspace. In so doing, Colombia has taken into account the measures recommended in the OEWG in which States have been invited to voluntarily share their opinions and national positions on this matter.

This position paper sets out the current view of the Republic of Colombia on the application of International Law in cyberspace and reflects many of the positions expressed by Colombia in various multilateral fora. It does not purport to convey an exhaustive analysis on the question, but rather to illustrate Colombia's general position on specific related issues.

This position paper was prepared by the Ministry of Foreign Affairs of the Republic of Colombia[1] in consultation with the Ministry of National Defense, the Ministry of Information Technologies and Communications, and the Office of the Presidential Advisor for Digital Transformation, as well as multiple stakeholders.

***

2. Application of International Law

Colombia considers it essential to achieving and maintaining international peace, stability and security, that States uphold their obligations under International Law. In that sense, all activities carried out by States in cyberspace must be and, in fact, are governed by International Law. This includes abiding by the principles and obligations enshrined in the Charter of the United Nations, such as sovereign equality, non-intervention in the internal affairs of other States, peaceful settlement of international disputes so as to preserve international peace and security, prohibition of 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. This also entails respect for human rights and fundamental freedoms.

Similarly, as set out below, Colombia considers that the behavior of States in the framework of ICTs must comply with the obligations, rules and principles of International Human Rights Law (IHRL) and International Humanitarian Law (IHL), including norms of Customary International Law. They also must comply with other applicable Customary International Law, such as the law of State responsibility, in their use of ICTs.

As reflected in the Annual Progress Reports of the OEWG,[2] the use of ICTs in future inter-State conflicts is increasingly likely, as is the continuing rise in incidents of malicious use of ICTs by State and non-State actors, including terrorist and criminal groups. Thus, advancing the debate on the implementation of IHL and other relevant rules and principles of Public International Law with regard to such cyberspace activities is a priority.

Moreover, the use of ICTs in a manner incompatible with the obligations incumbent on States under International Law and in contravention of confidence-building measures undermines international peace and security, trust and stability among States.

Cancillería

Colombia acts consistently with and respects the eleven non-binding voluntary norms[3] applicable in the cyberspace context, contributing to the achievement of the purposes of International Law, recognizing that both voluntary and binding regimes are essential to fostering a secure and stable cyberspace. These norms, although not obligatory in nature, constitute an important set of commitments dedicated to responsible State behavior, that complement and confirm certain rules of either Conventional or Customary International Law.

It is also important to highlight the need for enhancing and refining international cooperation in cyberspace guided by International Law, which Colombia understands as a global common- albeit man-made - by, *inter alia*, providing technical assistance and capacity-building, including the transfer of technology.

3. Sovereignty

In Colombia, the concept of sovereignty, understood as independence[4], is a foundational element of its foreign relations, as outlined in the Political Constitution[5]. Colombia understands sovereignty as encompassing both internal and external dimensions and conferring rights and imposing duties on States under International Law.

Colombia's Constitutional Court[6] has affirmed that the evolution of the notion of sovereignty does not detract from its core principles. The Court has highlighted three key dimensions: (i) sovereignty as independence; (ii) the understanding that undertaking international obligations does not undermine sovereignty, and sovereignty cannot be invoked to elude lawfully acquired obligations; and (iii) the principle of immediacy, according to which the exercise of sovereignty is subject to International Law without interference from other States. In this regard, Colombia acknowledges that sovereignty entails both rights and duties and is susceptible to violations that may constitute international wrongful acts.

State sovereignty is enshrined in key international and regional instruments such as the United Nations Charter, the Charter of the Organization of American States, and the Constitutive Act of the African Union, and has been further reinforced by judicial decisions from institutions such as the International Court of Justice, as a cornerstone of International Law.

As such, Colombia agrees with the conclusion contained in the report of the UN GGE[7], that Sovereignty and related applicable international rules and principles are applicable to the conduct of ICT-related activities by States and to their jurisdiction over ICTs infrastructure within their territory.

Thus, States exercise jurisdiction over ICTs infrastructure within their territory by, inter alia, establishing policies and laws as inherent functions of a State, as well as the necessary mechanisms to protect ICTs infrastructure within their territory from ICT-related threats.

Notwithstanding the above, Colombia recognizes the special characteristics of cyberspace and the particular challenges it poses to the application of the principle of Sovereignty. The aforementioned presents a significant challenge, that involves striking a delicate balance between national sovereignty and the need for cooperation and adherence to international norms, particularly in the cyber domain, where national and global interests often come into conflict. In this context, States need to further develop their legal views on how sovereignty applies in the cyber context, particularly in instances involving multiple jurisdictions at play and where the territorial component is absent or complex.

4. Prohibition of Intervention

The obligation of non-intervention, a principle of Customary International Law, prohibits States from coercively interfering in the inherent functions of the State[8], such as their political, economic, or social systems and foreign policy.

An act, including a cyber operation, that affects matters within a State's "domaine réservé"[9] and is coercive[10] in nature may violate the principle of non-intervention[11].

In accordance with the principle of non-intervention, States should not intervene directly or indirectly in the internal or external affairs of another State, including through ICTs. Such would be the case, for instance, of interference with the electoral systems of another State, or cyber activities directed at interfering with the operation of the systems of public agencies or institutions in another state.

5. Due Diligence

Arising from the principle of Sovereignty of States, the obligation of Due Diligence has been recognized by instances such as the International Court of Justice in the Corfu Channel case[1]. Due Diligence mandates States not to knowingly allow their territory to be used for acts contrary to the rights of other States, and to take all feasible measures to prevent and mitigate activities that affect the rights of other States and produces serious adverse consequences for them. Colombia considers that under International Law, this duty also applies in cyberspace.

In this regard, Colombia invites States to take appropriate measures to protect their Critical Infrastructure from ICT-related threats and to ensure that their territory is not used by non-State actors to commit unlawful acts.

Cancillería

Colombia also considers that States should encourage responsible disclosure of ICTs vulnerabilities and take appropriate measures within their jurisdictions and through international cooperation to ensure the integrity of the supply chain and to prevent the proliferation of malicious ICTs techniques and tools or hidden and harmful functions.

However, Colombia shares the view that the obligation of Due Diligence requires consideration of the technical, political and legal capacities of a State.

6. Peaceful Settlement of Disputes

Colombia considers that in the context of ICTs, States Parties to any international dispute that may endanger the maintenance of peace and security, or in case of disagreements on the application or interpretation of International Law, must first seek a resolution by the peaceful means set out in Article 33 of the Charter of the United Nations[13], namely: negotiation, investigation, mediation, conciliation, arbitration, judicial settlement, recourse to regional organizations or arrangements, or other peaceful means of their own choice. This obligation is not absolute and does not preclude other international legal obligations or rights, such as the fundamental right to self-defense. The foregoing is based on the obligations arising from Article 2(3) and Chapter VI of the Charter of the United Nations[14].

7. International Human Rights Law

International Human Rights Law applies to activities in cyberspace. State's initiatives established for the purpose of guaranteeing the security of information and communication technologies, as well as all actions in cyberspace, must respect human rights and the fundamental freedoms set forth in international instruments, such as the Covenant on Civil and Political Rights, the Covenant on Economic, Social and Cultural Rights, the American Convention on Human Rights, and the Universal Declaration of Human Rights, and in Customary International Law.

In addition to the above, Colombia believes that in order to ensure the safe use of ICTs, States must comply with Human Rights Council Resolutions 20/8, 26/13 and 47/16 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly Resolutions 68/167, 69/166, 77/211 and 75/176 on the right to privacy in the digital age, in order to guarantee full respect for human rights.

Furthermore, given certain practices, Colombia believes it is essential to recognize the unique challenges and vulnerabilities faced by women and other SOGIESC[15]-based marginalized groups online. The recognition of these challenges includes addressing, for instance, gender-based violence, digital harassment, and the gender digital divide. Therefore, mainstreaming a gender-responsive perspective in all relevant efforts ensures that international legal frameworks are inclusive and equitable, safeguarding the rights of all individuals. Colombia understands it is also necessary to acknowledge the human rights that are often affected by cyber activities including, but not limited to, the right to privacy and the right to freedom of opinion and expression.

8. International Humanitarian Law

Given the unique challenges and realities Colombia has faced throughout its history, IHL constitutes a field of particular relevance of International Law for our Country, considering its application is crucial to ensuring the protection of civilians and the effective regulation of armed conflicts.

IHL applies in situations of armed conflict whether international or non-international in character, and to all parties to a conflict[16]. In Colombia's view, IHL and its principles, namely humanity, necessity, proportionality and distinction, apply to States' use of ICTs in armed conflict.

Critical Civilian Infrastructure that enables the delivery of essential services is increasingly dependent on digitized systems. The preservation of such infrastructure and services from cyberoperations or incidental damage is vital to protecting the civilian population. It is necessary to build common understandings regarding what actions or conducts involving the use of ICTs or carried out in cyberspace, are prohibited, and how civilians and civilian objects can best be protected in times of armed conflict.

IHL provides specific protection to certain infrastructure and services, such as medical services, humanitarian operations, cultural property, the natural environment, works and installations containing dangerous forces, and objects indispensable to the survival of the civilian population, regardless of the type of operation involved.

8.1. Protected Objects

The question of what constitutes a protected object under IHL is also of utmost importance. Cyber operations against civilian data can have serious consequences for civilians, which should be addressed and discussed within the framework of IHL. However, Colombia considers civilian data to be generally protected from direct cyber operations, unless in the framework of IHL implementation, it becomes a legitimate military objective.

8.2. On the Notion of Attack

The definition of "attack" is of central importance for the application of IHL. States need to continue developing their legal views to clarify the notion of "attack" under IHL in the cyber context.

However, Colombia considers that in the context of cyberspace, the IHL notion of "attack" must be understood as defined in Article 49.1[17] of the Additional Protocol I to the Geneva Conventions.

It is now widely accepted that, in the cyber context, the notion of "attack" includes cyber operations reasonably expected to result in the death or injury of persons, or the destruction of or damage to objects. Notwithstanding the foregoing, opinions are divided as to whether operations that result only in a loss of functionality of the targeted system or object, without causing physical damage, constitute an attack under IHL. In that sense, there is a need to clarify the point (in terms of duration and nature of the loss of functionality caused) at which a cyber operation constitutes an attack.

Nevertheless, in terms of assessing a given "attack" in the context of cyberspace, Colombia currently identifies a cyber operation as an "attack" if it can be reasonably expected to cause injury or death to persons or damage or destruction to objects, including those causing loss of functionality without direct physical damage

Furthermore, in Colombia's view, for the purposes of the notion of "attack", cyber operations can damage objects in at least two ways. First, they can affect the provision of services to civilians, for example, cases of cyber operations against power grids and the health sector or aimed at disrupting the logistics involved in the transport and delivery of humanitarian aid. Second, they can cause physical damage to the infrastructure itself.

8.3. Protection and Participation of Civilians

Colombia considers it is necessary to take into consideration all existing rules of IHL, including the principles of military necessity and humanity, and all other measures necessary to protect the civilian population.

In this regard, it is relevant to analyze the specific impacts that cyberoperations may have on people in vulnerable situation, such as inter alia children, women, and the LGBTQ+ / SOGIESC community, under the applicable rules of IHL.

Notwithstanding the foregoing, a detailed legal analysis is also called for on the implications of the involvement of civilians in the planning and execution of cyber activities or operations, to find common understandings of when their conduct might amount to a direct participation in hostilities.

8.4. Precaution

In accordance with the rules of IHL, the planning and execution of lawful cyber operations must be carried out in a manner that respects the principle of precaution[18] in order to avoid and in any case minimize incidental loss of civilian lives, injury to civilians or damage to civilian objects.

9. Threat or Use of Force

In their use of ICTs, and in accordance with Article 2, paragraph 4 of the Charter of the United Nations[19], States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations.

It is Colombia's position that certain cyber operations could amount to a threat or use of force. However, several questions on this issue remain open and need to be further addressed by States, particularly those related to the threshold of what constitutes force in cyberspace.

10. State Responsibility

Internationally wrongful acts committed by a State, according to the criteria of Customary International Law on State Responsibility reflected by the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), are understood as those actions or omissions attributable to a State under International Law and which constitute a violation of an international obligation of the State.

Therefore, Colombia considers that internationally wrongful acts committed in cyberspace or by means of ICTs by a State against other State(s), by action or omission, engage its international responsibility. Colombia, however, acknowledges that in practice, invoking the responsibility of a State for an internationally wrongful act, involves complex technical, legal and political considerations[20].

11. Attribution

Colombia considers that the principle of State Responsibility applies in the context of cyber operations and, therefore, States may be internationally responsible if any State organ, or any person or entity with legal competence to exercise authority on behalf of the State, or any person or entity acting under instructions, direction or control from a State authority, has carried out cyber operations in breach of the State's international obligations.

Colombia is aware that limitations from a technological standpoint are challenging given that these activities are often conducted by third parties (via proxies or non state actors), which may make it difficult to attribute responsibility to a given State.

Despite the inherent difficulty in attribution and consequently determining the international responsibility of the State in the event of a cyber operation, the State that considers itself affected, before proceeding to take countermeasures, should take all necessary actions to identify the origin of the cyber activity when attributing responsibility to a State, in accordance with testing standards and international cooperation mechanisms for the attribution of attacks.

12. State's Responses and Circumstances Precluding Wrongfulness

States may react to cyber activities or operations conducted by another State with actions that would otherwise be contrary to their international obligations, but the wrongfulness of which is precluded under International Law due to specific circumstances.

This is without prejudice to the necessity of initially seeking resolution in accordance with established principles and norms of International Law. Even where there may be sufficient grounds for attributing responsibility to a State, the affected State is encouraged to first pursue direct dialogue with the allegedly responsible State or, if appropriate, engage a third State to facilitate such discussions, in line with the principles of negotiation, mediation, and peaceful resolution as prescribed by the Charter of the United Nations.

12.1. Self-Defense

A State targeted by a cyber activity or operation that amounts to an armed attack may invoke its inherent right of self-defense, pursuant to the customary right to self-defense, as outlined in Article 51 of the UN Charter[21] and reflected in Article 21 ARSIWA[22].

It is the view of Colombia that, when exercising the right to self-defense in response to a cyber activity or operation that amounts to an armed attack, States must uphold the thresholds and limitations outlined in Article 51.

12.2. Countermeasures

In accordance with the principles of International Law, in the event that a State is found to be responsible for a cyber operation that amounts to an internationally wrongful act, the affected State is entitled to adopt countermeasures[23] to ensure the cessation or reparation of the unlawful conduct by the former.

These countermeasures must be proportionate to the damage suffered and may be taken in the context of cyberspace or outside it.

In case of breach of erga omnes obligations, States other than the injured State may also take countermeasures against the State responsible for the cyber operation.

12.3. Retorsion

States may respond to unfriendly or unlawful acts conducted by other States in the context of cyberspace by adopting measures known as retorsions. These actions, although potentially perceived as unfriendly do not violate International Law. Examples of retorsions include severing or limiting diplomatic relations and imposing trade restrictions.

Retorsions may also include cyber-specific actions, such as issuing warnings to cyber operatives from another State.

13.Further Developments

In cyberspace, new developments continue every day and, therefore, the requirements for States in relation to their application of International Law continue to evolve. For instance, the emergence of “virtual”, “digital” or “data” Embassies, implies the necessity for States to agree on the specific circumstances under which international diplomatic immunity apply to them.

14. Final Remarks

This position paper highlights the current views of the Republic of Colombia on how International Law applies to the use of ICTs by States. Given the scope of International Law, only certain salient aspects are covered, particularly those of specific relevance to our State due to its history, context, and other key factors, where Colombia has more elements to develop its position at this time.

Colombia continues to analyze this issue and will keep contributing further insights on the application of International Law to cyberspace, including through the issuance of dedicated sections on specific topics or the development of concrete examples.

Finally, Colombia believes that any ambiguities on how International Law applies in the cyber context should be addressed through international dialogue and cooperation engaging the combined efforts of States, international organizations, civil society and academia.

***

FOOTNOTES

[1] In the preparation of this position paper, the Republic of Colombia considered various sources including, inter alia, the work of the past and current UN Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG) and the past UN Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (GGEs), as well as the Tallinn Manual and the Cyber Law Toolkit.

[2] Para. 13 of the 2024 Progress Report

[3] The United Nations Norms of Responsible State Behaviour in Cyberspace.

[4] Island of Palmas (Neth. v. U.S.), 2 RIAA 829, 838 (Perm. Ct. Arb. 1928).

[5] Article 9. Colombia's Political Constitution

[6] Judgment C-621/01 by the Constitucional Court issued on June 13th of 2001

[7] GGE Final Report. 2013.

[8] Internal or external affairs of other States.

[9] Areas where the State is free to decide, for example, like national elections or foreign policy,

[10] Coercion can be understood in two ways: either as an act designed to compel a State to change its behavior or as an act that deprives a State of its control over these matters. While military interventions are clear cases of coercion, non-forcible interference, such as economic or political coercion, is more complex and context-dependent, with cyber operations often cited as an example.

[11] This principle was outlined by the International Court of Justice Case Nicaragua v. USA

[12] Judgment of the International Court of Justice. (United Kingdom of Great Britain and Northern Ireland v. Albania). 1949.

FOOTNOTES

[13] Article 33 of the Charter of the United Nations:
1.“The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.
2.The Security Council shall, when it deems necessary, call upon the parties to settle their dispute by such means.”
[14] Article 2(3) of the Charter of the United Nations:
“The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.
(3) All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”
[15] SOGIESC: Sexual Orientation, Gender Identity and Expression, and Sex Characteristics
[16] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para. 86; "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."
[17] Article 49 — Definition of attacks and scope of application
1. “Attacks” means acts of violence against the adversary, whether in offence or in defence.
[18] In accordance with Article 57 of Additional Protocol I to the Geneva Conventions.
[19] Article 2(4) of the Charter of the United Nations:
“The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles:
(4)All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

FOOTNOTES

[20] (GGE 2021)

[21] Article 51 of the Charter of the United Nations

"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."

[22] Article 21 of the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts:

"The wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of selfdefence taken in conformity with the Charter of the United Nations."

[23] Colombia understands countermeasures as those measures, that would otherwise be contrary to the international obligations of a State, taken by an injured State in response to an internationally wrongful act, to procure cessation and reparation from the responsible State".

***

Cancillería

BIBLIOGRAPHY

- Additional Protocol I to the Geneva Conventions.
- Charter of the Organization of American States.
- Colombia's Constitutional Court. Ruling C-621/01. (2001).
- Colombia's Political Constitution.
- Constitutive Act of the African Union
- Cyber Law Toolkit https://cyberlaw.ccdcoe.org/wiki/Main_Page
- International Court of Justice. Corfu Channel Case (United Kingdom v. Albania. (1948).
- International Court of Justice. Nicaragua v. United States Case. (1986).
- International Court of Justice. Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons. (1996).
- International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (2001).
- Open Ended Working Group. Final Report. (2022).
- Oxford Institute for Ethics, Law and Armed Conflict (ECLAC)
- Permanent Court of Arbitration. Island of Palmas (Netherlands. v. United States.). (1928).
- Tallinn Manual on the International Law Applicable to Cyber Warfare. (2013)
- United Nations Charter
- United Nations General Assembly Resolutions (68/167, 69/166, 77/211, 7 5/176, 75-240)
- United Nations Human Rights Council Resolutions (20/8, 26/13, 47/16)
- United Nations Group of Governmental Experts. Final Report. (2021).

***

Cancillería