**ITU SECOND ONLINE CONSULTATION ON THE DRAFT GUIDELINES FOR THE UTILIZATION OF THE GCA**

DEAR ITU SECRETARIAT,

Regarding to the ITU SECOND ONLINE CONSULTATION ON THE DRAFT GUIDELINES FOR THE UTILIZATION OF THE GCA of baseline positions about Consultation Paper: my feedback and general comments in public consultation are following and I reaffirm my full support for the joint decisions from the ITU members and all regulatory bodies in United Nations.

January 12, 2021.

**ANDREA ROMAOLI GARCIA**

**INTERNATIONAL TAX LAWYER and LEADER OF GLOBAL COMPACT FOR WEPS BY UN WOMEN**

**ITU-WHO TOPIC DRIVER IN AI4H OPEN SOURCE PROJECT**

**andrea.garcia@fibree.org**

[**https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/opencode.aspx**](https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/opencode.aspx)

[**https://www.weps.org/company/romaoli-international-management-consultancy**](https://www.weps.org/company/romaoli-international-management-consultancy)

**MALTA**

**PRELIMINARILY - LEGAL JUSTIFICATIONS**

United Nations is the guardian and responsible for the guarantees that prevent human rights violations. Thus, United Nations resolutions will be considered binding in Member States depending on the nature of the resolution.

Onto this scenario the International Telecommunication Union is a specialized agency of the United Nations responsible for all matters related to information and communication technologies which formally entered into force on 1 January 1949.

To understand the limits of nature of resolution is necessary the knowledge on the source and powers of international laws and the scope of ITU -UN in matters of information and communication technologies.

First, international laws embodies a legal system and because it is a system the legal interpretation is a consturctive process that serves to provide answers to ITU Second Open Online Consultation on the Draft Guidelines for the Utilization of the Global Cybersecurity Agenda (GCA). ***This submission suggest a recommendation in the Draft Guidelines that strengthen the relevance of ITU resolutions/decisions.***

**GENERAL COMMENTS**

In terms of consturctive process onto proper legal interpretation this submission discuss the UN and ITU powers and limits also the source of international laws since sovereignty and Cybersecurity relates to International Laws due to the Guideline on 2.9. H at PILLAR 1 is relevant to issues about ***sovereignty and access to the content of encrypted communications***.

In terms of consturctive process onto proper legal interpretation this submission discuss the UN and ITU powers and limits also the source of international laws since sovereignty and Cybersecurity relates to International Laws.

The rules of international law come from treaties and customary international law that is created by States. Also the International law has 2 coverings: a) Public International Law; b) Private International Law. The Public International Law covers rules, laws and customs that is applied to governs the International affairs among the nations and their citizens.

In terms of the powers of United Nations and ITU, the UN is responsible for Public International Law and somecases will deal disputes between private citizens among the nations. This power already was gratend by the Member States that assigned to The Universal Declaration of Human Rights. Since, ITU is a specialized agency of the United Nations responsible for all matters related to information and communication technologies wich it means ITU has the same UN's Power. The only difference remains on the subject: ITU has limited subject on content of information and communication technologies. Regulations, rules, standards, protocols is among ITU's content in matters of information and communication technologies. It means laws. In sum, ITU is entitled by the UN Member States for build the regulations, rules, standards, protocols and laws on matters of information and communication technologies.

In terms of the application of International Law to States Cybersecurity and Sovereignty it is subject to statesóbligations under international human rights law: The Universal declaration of Human Rights and its legal system.

It is in accordance of the Chatan House[[1]](#footnote-1):

"States have the right to exercise their sovereign powers over cyber infrastructure in their territory exclusively and independently, as in the non-cyber context. These powers over cyber infrastructure are subject to states' obligations under international human rights law[...]"

The legal meanful is: the States does regulation on nacional territory and its citizens and the international law will deal on international space since it respects the **HUMAN RIGHTS** and **PRINCIPLES OF SOVEREIGNTY** such as **NON-INTERFERENCE** also **INTERNATIONAL COOPERATION** that ensures the security against unlawful invasions and the right to the act through international courts to reestablish the **PEACE AND JUSTICE**.

*Sovereignty* relates to territorial authority that involves a range of rights wich its limits is about the relationship of a State does in its territory also it excludes all other states at this scenario. When a State does relations with other States has a friendly approach promoted by international laws under 3 fundamental rights: **JURIDICAL EQUALITY, TERRITORIAL INTEGRITY** and **FREEDOM AND POLITICAL INDEPENDENCE**.

This rules drives the limits to impose the violation of Sovereignty and the air is included in territorial integrity.

In terms of cyberspace, the interactions happens virtually through transmission of data, signalling and sharing contents between physical devices.

Despite the Cyber infrastructure has servers located in particular territory it doesn't means interactions in a particular territory. Indeed the interactions in cyberspace is deterritorialized that happens in dependency physical space.

Thus, the principle of sovereignty applies in states's cyber activities. It means that States must exercise their power of sovereign over cyberspace in their territory exclusively. Following the international legal system that State Members assigned along to UN, these powers of sovereign over cyberspace are subject to States'obligations under international laws and should respect the human rights law.

Considering that States remotes intrusions happens through the physical and air lines, a cyber remote intrusion should be treated at the same way that territorial sovereignty. It concludes that in international space the international legal system and international laws is applied.

There is no justification for a different legal interpretation since the **PRINCIPLE OF NON-INTERFERENCE** is among international legal system wich it garanthees that unlawful interations will be under suits in international courts.

It was expressed in ***Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information and Telecommunications*** in the Context of International Security by **UNGA 2015** [[2]](#footnote-2)**:**

"In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;" ( ***UNGA Report July 2015, 28 b, sessions A70/174***).

**GUIDELINES TO UTILIZE PILLAR 1 - LEGAL MEASURES - 2.9.H**

Considering the expressed content:

"2.9 Given the rapid advancements in technology, measures taken by organizations and countries need to evolve to keep pace with the rate of change. This brings new complexities to the challenge of cybersecurity, requiring close examination from a variety of different perspectives. In this context, proposed guidelines for utilization of Pillar 1 are set out below:

h. Noting that the principle of state sovereignty applies in cyberspace, Member States are encouraged to explore mechanisms that protect the fundamental rights and safety of citizens while also facilitating lawful access to the content of communications where end-to-end encryption has been implemented."

The **Guideline on 2.9. H at PILLAR 1** brings security to cyberspace and it contributes to international collaboration.

**INTERPOL[[3]](#footnote-3)** has strengthening border security through enhanced frontline collaboration which many countries agree on to establish ***mechanism applying the international laws[[4]](#footnote-4)*** in cyberspacy to generate security to all nations. Then, ***Guideline on 2.9H at PILLAR 1*** is alligned to international regulatory field also it contributes to States Members reach the Public Interest to their citizens by generating a full covering: national and international security.

ACCESS TO THE CONTENT OF ENCRYPTED COMMUNICATIONS

The content of Guideline on 2.9. H at PILLAR 1 is in Compliance to national and international regulatory system since the non-interference principle is among international legal system wich it garanthees that unlawful interations are prohibited also will face suits in international courts. Wilful misconduct isn't supposed. Wilful misconduct should be proved. It means that the ***ITU Guideline on 2.9H at PILLAR 1*** is in Compliance.

The protocols will build the technical distintions that appears as necessary due to is the proper legal form. Guidance provides advices, improvements and ways to develop potentials.

The protocols will build the technical distintions that appears as necessary due to is the proper legal form. Guidance provides advices, improvements and ways to develop potentials.

**CONCLUSION**

For all those reasons the **Guideline on 2.9. H at PILLAR 1** **is in Compliance to national and international regulatory system also it collaborates to international cooperation for the utilization of the GCA as far as the recommendation is in accordance of ITU PLENIPOTENTIARY RESOLUTION 130 due to ITU has power to do regulation on international space.**

This is my legal comment.

**ANDREA ROMAOLI GARCIA**

**ANDREA ROMAOLI GARCIA**

**INTERNATIONAL TAX LAWYER and LEADER OF GLOBAL COMPACT FOR WEPS BY UN WOMEN**

**ITU-WHO TOPIC DRIVER IN AI4H OPEN SOURCE PROJECT**

**andrea.garcia@fibree.org**

[**https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/opencode.aspx**](https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/opencode.aspx)

[**https://www.weps.org/company/romaoli-international-management-consultancy**](https://www.weps.org/company/romaoli-international-management-consultancy)

**MALTA**

1. <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace> [↑](#footnote-ref-1)
2. <https://digitallibrary.un.org/record/799853?ln=en> [↑](#footnote-ref-2)
3. <https://www.interpol.int/ar/1/1/2017/Strengthening-border-security-through-enhanced-frontline-collaboration> [↑](#footnote-ref-3)
4. <https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services> [↑](#footnote-ref-4)