



University for Peace



Costa Rica, 24 March 2022

University for Peace Statement Addressed at the First Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Thank you, Mr. Chairman / Madame Chairperson,

The University for Peace, established by the United Nations General Assembly Resolution 35/55 of December 1980, welcomes all delegations that contribute to the debate on the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

The University for Peace believes that an international convention must be visionary, reflecting what are our main current challenges and solutions but also to comprehend what will be the scenario we will all face in the coming years. In this regard, a harmonization of national, regional, and international frameworks for data protection and secure communications technology is necessary to provide the world with adequate norms and standards to protect citizens from malicious actors looking to wreak havoc on government and individual property. The terms, objectives, and scope of the convention based on national and global challenges to provide the world with a relevant standard on protecting technologies and property in the digital sphere. The University for Peace recognizes harmonization and standardization of terms, objectives, and scope are at the center of the multilateral debate to achieve consensus on the structure of the convention.

The University for Peace acknowledges that this convention will be an important legal source to improve and protect citizen guarantees for the right to freedom of expression, as well as freedom of the press, as we recognize the importance of journalists in the unraveling of illicit schemes across the world journalists and media outlets to counter the use of Internet-based platforms for criminal purposes. While citizens use information and communication technologies, particularly social media, to disseminate discriminatory speeches, leverage criminal activities, and conduct campaigns of misinformation, along with other forms of prohibited content, the challenge is to limit the negative effects and misuses of this medium without infringing upon individuals' right to express themselves freely.



University for Peace



Mr. Chairman / Madame Chairperson

The University for Peace created, in August 2021, the Chair on Countering Illicit Trade and Preventing Transnational Organized Crime. This Chair reflects an innovative approach to organized crime from a perspective of state fragility. While organized crime benefits from vulnerabilities on the economic, political, social, environmental, and security spheres, we also know that illicit trade and organized crime threaten state stability, weaken institutions, and corrupt government structures.

In this context, the University for Peace turns its attention and reinforces its commitment to the study of organize crime in the peacebuilding and conflict resolution fields, considering the impact of cybercrime and related illicit activities, mainly those crimes that directly affect citizen security. The COVID-19 pandemic has shed light on the evolution of criminal organized groups and their illicit practices. Such adaptability is an issue of concern for the convention since it should function as a guide in the area of information and communication technologies.

Within the scope of the First Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, the University for Peace would like to highlight two main issues to be considered as part of the General Provisions.

First, the convention should build upon existing regional and international instruments on data protection. Although some of these instruments are not legally binding, they provide a framework for the convention regarding terms, scope, and objectives it should address. The following instruments adopt focus areas that the convention should consider for its General Provisions:

- i) *The Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*;
- ii) *the Council of Europe Convention 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data*, as amended in May 2018;
- iii) *the European Union General Data Protection Regulation* and *the European Union Law Enforcement Directive*;
- iv) *the 2004 Asia-Pacific Economic Cooperation Privacy Framework*;
- v) *the Economic Community of West African States Supplementary Act on Personal Data Protection* from 2010; and
- vi) *the African Union Convention on Cybersecurity and Personal Data*.

These instruments focus on the definition of crucial terms that should serve as a guide for the convention to comprehend, more fully, the challenges it addresses. While terms included in the instruments differ slightly, they all embrace similar concepts such as *personal data*, *data processing*, *controller*, *recipient*, *processor*, and *sensitive data*, among others.



University for Peace



Two of these concepts are particularly relevant for broadening the scope of the convention at hand: *transborder flows of personal data* and *publicly available information*. Since the convention aims to counter the use of information and communications technologies for criminal purposes, it is essential to consider that crimes committed with the use of information and communications technologies are transnational, meaning that they are illicit activities orchestrated and carried out by organized criminal groups. The concept of *publicly available information* addresses the different levels and actors involved in the domain of information and communication technologies, such as governments, journalists, and legal actors, who make information public, as required by the law. Additionally, the convention should consider changes in technological innovation and their influence on the concepts the document at hand adopts. This might require the use of more loose terminology at times.

Mr. Chairman / Madame Chairperson

The second aspect the University for Peace would like to address is related to the scope of the convention. To achieve the aim of the International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, we must garner support from the private sector on this matter. Since each state party to the convention will be responsible to protect personal data rights, it is important to consider the way in which the private sector manages consumer information in its databases.

In times of technological innovation, including the fourth industrial revolution, this convention presents itself as a valuable tool to address the invisible threats that impact our daily lives, from transnational fraud to unauthorized use of information for political purposes. The use of personal information not agreed upon by individuals is a crime and a violation of human rights, information security and human security.

I conclude, Mr. Chairman / Madame. Chairperson, affirming that, at the University for Peace, we believe that promoting media literacy and incorporating obligations aimed to identify stakeholders, prevent the use of communication technologies for criminal purposes, and design mechanisms to increase cooperation between states, software developers, internet providers, and the media will be an important step to frame the discussions and the final draft of the convention.

Thank you very much, Mr. Chairman | Madame Chairman