



## WORLD BANK COMMENTS

TO THE SIXTH SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

August 15, 2023

# 1. Overview

The World Bank Legal Vice Presidency appreciates the opportunity to submit its comments on the draft text (A/AC.291/22) for a **Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes** to the Sixth Session of the Ad Hoc Committee (AHC) in advance of its meeting in New York, 21 August – 2 September 2023. The comments, specifically focusing on Chapter V, are grounded in the World Bank's unique position and experience as a leading multinational development bank. Insights are drawn from our existing and ongoing cyber capacity-building operations, reflecting our specialized understanding of the subject matter.

# 2. The World Bank Background

The World Bank is an international financial institution and specialized agency of the United Nations that provides financial and technical assistance to developing countries for development and capacity-building projects. The World Bank's goals are to end extreme poverty and promote shared prosperity in a sustainable way.

Collaboration with other international organizations, governments, the private sector, and civil society enables the World Bank to pursue these goals with a multifaceted approach, addressing challenges such as infrastructure development, education, health, agriculture, and environmental sustainability. The World Bank's focus spans beyond traditional development areas and extends to areas like digital development, where building capacities to combat cybercrime is an essential component.

## Overview of World Bank Operations in Cybercrime

**Financial Support and Funding:** The World Bank extends financial support to countries to develop and implement multifaceted aspects of the enabling policy, legal and technical framework essential

for digital development, including combatting cybercrime. This support encompasses strategies, infrastructure, and legal frameworks. The financial support is provided through grants, loans, and credits, specifically aimed at funding projects that enhance digital security.

**Technical Assistance and Capacity Building:** The World Bank offers technical assistance support through its financing activities as well as in the form of expertise which encompasses the design of cybersecurity policies, laws, and institutional/governance structures. Training programs are also provided to develop skills among policymakers, legislators, law enforcement, the judiciary, and other stakeholders in cybercrime prevention, detection, and response.

**Research and Knowledge Sharing for Capacity Building:** The World Bank engages in research and analysis on trends, risks, and best practices in combatting cybercrime. This research informs policy development and provides insights into the global landscape of cybercrime. Knowledge-sharing platforms – with many organizations present in these discussions - are facilitated to promote the exchange of experiences and best practices among countries, international organizations, and the private sector.

**Collaboration with International and Regional Partners:** As part of that knowledge sharing and capacity building, the World Bank supports a multi-stakeholder approach. We encourage collaboration with international organizations, governments, NGOs, CSOs, and private sector entities. We are proud to have worked with a number of UN organizations, international organizations, bar associations, and academia – again, many of which are participating in these discussions - in the publication of our Capacity Building Toolkit (available at: [www.combattingcybercrime.org](http://www.combattingcybercrime.org)). Additionally, the World Bank often works with regional organizations to tailor cybersecurity initiatives to specific regional needs and challenges.

**Focus on Inclusivity and Sustainability:** The World Bank emphasizes support for developing countries, where resources for combating cybercrime may be limited. Cybersecurity initiatives are aligned with broader sustainable development goals to ensure that digital development is inclusive, resilient, and supportive of economic growth.

## The World Bank's Combatting Cybercrime Toolkit

### Tools and Capacity Building for Emerging Economies

The World Bank's Combatting Cybercrime Toolkit, launched in 2017 in collaboration with participating organizations, including [Council of Europe \(CoE\)](#), [International Association of Penal Law \(AIDP\)](#), [International Telecommunication Union \(ITU\)](#), [Korea Supreme Prosecutors Office \(KSPO\)](#), [Oxford Cybersecurity Capacity Building Centre](#), [United Nations Conference on Trade & Development \(UNCTAD\)](#), [United Nations Interregional Crime and Justice Research Institute \(UNICRI\)](#), and [United Nations Office on Drugs & Crime \(UNODC\)](#), exemplifies the multi-dimensional nature of capacity building in the fight against cybercrime.

This initiative particularly highlights capacity building and its various dimensions. By fostering collaboration and focusing on the unique roles and expertise of different entities, the Toolkit promotes a comprehensive and nuanced approach to building capacity to combat cybercrime.

With the **second edition** of the Toolkit expected in 2023, the Toolkit underscores the complexity of the challenge and emphasizes the necessity for a coordinated, multifaceted, multistakeholder response that leverages the strengths and specializations of diverse participants in the global effort to combat cybercrime.

## 3. Comments on the Draft Text of the Convention

### **Maximize the Role of International Organizations and Relevant Stakeholders in Promoting and Developing Preventive Measures (Chapter V, Article 53)**

We welcome and support the reference to the role of international organizations in the field of prevention in Article 53. Preventive measures, paragraph 6, represents a forward-thinking approach to the prevention of cybercrime, emphasizing collaboration and flexibility.

### **Leverage Existing Frameworks for Technical Assistance and Capacity-Building Provided by International Organizations like the World Bank and Relevant Stakeholders (Chapter V, Article 54)**

We suggest amending Article 54, paragraph 8, to encourage States Parties to strengthen efforts to maximize the effectiveness of technical assistance and capacity-building through operational and training activities in international and regional organizations. The proposed amendment to article 54(8) is as follows:

“States Parties are encouraged to strengthen, to the extent necessary, efforts to maximize the effectiveness of **technical assistance and capacity-building** through operational and training activities in international and regional organizations and in the framework of relevant bilateral and multilateral agreements or arrangements.”

## 4. Rationale

### **Leveraging Specialized International Organizations**

Multi-stakeholder engagement enhances capacity building at all levels, leading to faster learning of lessons and more effective coordination. Such combined efforts grow synergies and avoid overlap, maximizing the impact of each organization's unique strengths.

## **Overcoming Limited Resources Through an Organized Approach and Coherent Strategy**

The biggest barrier to capacity building, particularly in the field of combatting cybercrime, is frequently limited resources. International organizations can mobilize additional resources, both financial and technical, to supplement domestic efforts. By leveraging their global networks and expertise, they can attract funding and support from various donors and partners. This targeted approach leads to more effective capacity building, as resources are deployed where they are most needed and can make a real difference in combating cybercrime.

## **5. Conclusion**

In conclusion, the involvement of international organizations in capacity building for cybercrime offers a multistakeholder solution to the problem of limited resources, particularly in developing countries. By mobilizing further resources, growing stakeholder engagement, and ensuring that resources are available and used impactfully, international organizations play a crucial role in enhancing the global fight against cybercrime. The World Bank lends its full support to the recognition of the role of international and regional organizations in promoting and developing preventive measures, as encapsulated in Article 53, paragraph 6 of the draft text of the convention, and suggests amending Article 54, paragraph 8 to overcome potential barriers to capacity building.

### **For Further Inquiries**

For further information, kindly direct your inquiries to the following contacts:

**Keong Min Yoon** (kyoon1@worldbank.org), **Counsel, Cybersecurity and Digital Infrastructure**

**Min Suk Kim** (mkim20@worldbank.org), **Senior Counsel**