



Statement

By Ambassador Mohamed El-Molla

Ambassador & Permanent Representative of Egypt in Vienna,

**To the Plenary Session of the Meeting of
the Ad Hoc Committee on Establishing
a Convention on Cybercrime**

New York - 28th of February, 2022

Check against delivery

**Madame Chairperson,
Esteemed Excellencies,
Distinguished delegates,**

At the outset, please allow me to express my happiness to see you Mme Chairperson and Algeria at the helm of this process. Egypt appreciates your efforts in leading these negotiations. The wisdom and expertise you have demonstrated throughout the year are truly commendable. I am also pleased to witness such strong engagement and active participation in today's meeting.

It is also both a pleasure and an honor to speak to you today at the commencement of what is considered as one of the most timely and foundational international undertakings in the past few years. It is not difficult to understand why it is of paramount importance to address this ever-growing problem at this critical juncture in time, to coordinate international efforts to ultimately prevent and combat Cybercrime. This is paramount, owing to the rapid increase of cybercrime globally, which was exacerbated by the COVID-19 pandemic.

Cybercrime rates have risen globally to concerning extent. Every 32 seconds, a hacker attacks someone online. In 2021 alone, over 60% of companies across the globe reported ransomware, phishing and social engineering attacks, resulting in considerable financial losses not only for the companies but also for entire economies. Several organized crime groups are now investing in cybercrime, seeing as it has become more lucrative than drug trafficking. Expenditure on cybersecurity prevention and containment measures is also on the rise, 2022 is expected to see a worldwide annual spending of nearly \$134 billion, a figure that is set to rise further.

The growing importance of unifying international efforts to combat cybercrime is demonstrated by the immeasurable financial losses that are incurred annually on a global scale. Estimates in this regard vary, nonetheless, they are nothing short of shocking; the most conservative studies conclude that close to 600 billion dollars, nearly one percent of global GDP, are lost to cybercrime each year. Other estimates placed the global financial losses due to Cybercrime in 2021 at 1 trillion dollars, with some even predicting that this number could grow per annum to 10 trillion dollars by 2025. These staggering figures, which are growing exponentially, could be devoted instead to achieving sustainable development on a global scale, especially for the Global South, including the African continent.

Nationally, Egypt has had its fair share of the burdens posed by Cybercrime. Over the past decade, my country witnessed numerous developments in this regard. The rate of Cybercrime in Egypt increased by about 190% from 2012 until 2017. Concurrently, Egypt launched an ambitious national strategy to digitally transform its government and fully digitize vital processes within it to tackle the rising phenomenon of cybercrime in a manner that allows a smooth digital transition; Egypt issued its first-ever Anti-Cybercrime law in 2018 (No. 175/2018), which adopted a comprehensive approach to tackle this issue. Egypt also issued a data protection law and launched a Cybersecurity national strategy.

In light of the aforementioned developments, Egypt believes it is necessary to attach the utmost importance to promoting international cooperation and harmonizing efforts to combat cybercrime. Egypt believes that these efforts should take place under the auspices of the United Nations, premised primarily on the respect for the principle of State Sovereignty, which should create an overarching international legal framework for States parties, as opposed to depending on stopgap regional agreements alone. Egypt has actively partaken in the UN process to elaborate an international convention on Cybercrime since its very inception, throughout three resolutions, studies, and the report of the UNGGE along the way. Egypt actively contributed not only to express its national interests and priorities but the aspirations of the African continent as a whole. I am therefore proud to reaffirm today that Egypt will continue to contribute constructively until our collective goal is achieved.

From this standpoint, I would like to elaborate further on Egypt's vision for the aspired international convention on Cybercrime. Firstly, Egypt believes that the upcoming process should focus mainly on building on our common international denominators with regards to the multitude of aspects of Cybercrime. Our purpose and object should be to find as many commonalities and intersections as possible that will help construct a unified approach to address issues that garner consensus. Egypt understands that the priorities and concerns of each state is inevitably going to differ, however, this does not negate the possibility of the existence of many points of convergence for all parties. It is these convergences that we must strive to discover, whether they pertain to the definitions, criminalization and legal procedures to combat cybercrimes or the establishment of certain mechanisms for international cooperation, capacity building and technology transfer. This confluence will ultimately help us devise common approaches to address issues that are of collective concern.

Accordingly, Egypt believes that it is vital to take into account the particularities and concerns of all states involved, especially considering the existence of a prominent national security component to cybercrime. While Egypt understands that internet governance, and by extension any international cybercrime framework, is a multi-layered multi-stakeholder process, we are confident that all States parties agree on the importance of preventing any interferences that undermine states' sovereignty or place asymmetrical obligations on States vis-à-vis their relationship with other stakeholders. Ultimately, this is a process that is designed to lead to an international agreement that principally will place obligations on States parties.

Furthermore, Egypt believes that the ultimate objective convention should be to enhance international cooperation in the field of the use of information communication technologies for criminal purposes. This is intended to prevent any measures that could undermine the safety and confidentiality of data. Additionally, the convention should collectively criminalize the use of ICTs for criminal purposes, facilitate means of investigations and the pursuit of perpetrators. An element about the seizure and recovery of financial assets obtained through cybercrime should also be incorporated. Most importantly, the convention should provide sufficient jurisdiction to combat cybercrime effectively through establishing international cooperation measures that facilitate the discovery, investigation, pursuit, and even extradition of cybercriminals.

The scope of the convention should include provisions to ensure the establishment of legal jurisdiction not only over the territory of each state party but also provisions to allow for investigations of trans-national cybercrimes that may take place in different territories. As for definitions of Cybercrime within the convention, Egypt believes that States parties should work to elaborate unified definitions on core cybercrimes that are of common interest while recognizing that each state party is to complement the remaining crimes through its national laws and legislations. These core cybercrimes should include both computer-dependent crimes and computer-enabled crimes. The core cybercrime definitions should be comprehensive and diverse to ensure the effectiveness of the treaty, ranging from forgery, blackmail, and fraud to attacks on the critical infrastructure of states, sexual exploitation, money laundering, and cyberterrorism in addition to cybercrimes-related to international organized crimes.

Egypt also believes that internet service providers (ISPs) and other legal entities in cyberspace have several roles pertinent to combating cybercrime. The intended convention should also include an important component that outlines these roles while maintaining respect for data privacy and protection.

As for international cooperation measures, Egypt believes that each state party should act in good faith to facilitate international cooperation to the maximum possible extent, with speedy responses and reciprocity being the gold standards applied in this regard. Egypt believes that information sharing and legal assistance under the auspices of the convention, while a complex matter, contributes to the prevention of cybercrime and aids in its investigation and the pursuit of cybercriminals.

Facilitating mutual assistance should also be at the heart of the convention. In this regard, mutual assistance should be encouraged to the maximum possible extent, contingent upon the sovereign decision and the internal laws of each state. The convention should establish a fast, responsive, and confidential means of direct communication between States parties to be established via dedicated national contact points, or even through Interpol, to facilitate mutual assistance in combating cybercrime and collecting evidence. There are several important caveats and safeguards that Egypt believes should be placed in this regard, namely allowing each state to accept or reject a request for assistance while maintaining the confidentiality of the requesting state.

Egypt believes that it is important in this respect to encourage States Parties to assist other requesting states to expeditiously halt attacks in the cases of urgent and serious cybercrimes. While the choice of accepting assistance remains a sovereign decision of each state, Egypt believes States should be encouraged to explain reasons for rejection should that occur. Egypt also believes that each State party should establish a specialized entity working around the clock to ensure the provision of immediate assistance to other states for the purposes of investigations or collection of cybercrime evidence. This exchange can also be expanded to include providing legal consultations and the provision of information that can lead to the detection of the whereabouts of perpetrators.

With regards to technical assistance and capacity building within the framework of the future convention, Egypt believes that it is vital for States parties to provide the utmost technical assistance possible. The transboundary nature of cybercrime requires the creation of internationally qualified cadres across the globe to combat and stop cybercriminals.

Accordingly, developing states and in Egypt's case, fellow members of the African continent should be accorded due care and priority concerning capacity building and technical assistance. This should include training of personnel and transfer of technology to developing states as well as the exchange of best practices and lessons learned. Egypt believes that states parties should also aid one another in providing data and statistics about the latest trends and modus operandi of cybercriminals in order to contribute to preventive efforts in addition to periodical updates on the best methods of cybercrime investigation, electronic forensics, and evidence gathering.

Egypt ultimately believes that more developed states in the field of combating and preventing cybercrime have an additional burden to provide technical assistance to developing states in this regard. However, given the transboundary nature of cybercrime, Egypt believes that this burden will yield valuable benefits to the international community at large, as developing states are empowered to track and locate cybercriminals within their borders.

Moreover, Egypt believes that it is imperative to enshrine within the intended treaty a governing principle that allows States parties to make reservations that do not conform to their national views or present challenges that they deem to be unfeasible. It is important in this regard to take stock of the multiple existing treaties on cybercrime, which enable states to make decisions regarding ratification according to their priorities. On the other hand, States parties should work to ensure that reservations to the convention do not end up nullifying or undermining its object and purpose.

In conclusion, Madame President, Egypt believes that this process, upon which we are about to embark, presents a vital opportunity at a critical moment to the international community to collectively address a global problem that can only be remedied through an innovative global solution. The lack of physical borders in cyberspace necessitates us to bring about a paradigm shift in how cybercrime is tackled, which should eventually culminate in the adoption of a responsive and swift international approach that is premised on a common vision far removed from dialectical redundancies and political differences.

Thank you Madame President.