LEINOTECH
Legal Innovation Technology
Andisheh Varzaneh Fanavari Tanzimi

Andisheh Varzaneh Fanavari (Leinotech) Statement on General Provisions for the Second Session Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Islamic Republic of IRAN - Private Sector

6 JUNE 2022

According to our proposed detailed Draft (including General Provisions, Provisions on Criminalization, Procedural Measures and Law Enforcement) that has been previously submitted on 8 April 2022, the principles on the chapter of General Provisions are as follow:

1. The main strategy of the Convention is institutionalization of "Universal Cybercrime Policy", which means the application of all the preventive measures, and the judicial, regulatory and trade union responses to cyber threats, and the violation of its norms. Therefore, the Convention must be able to provide reasonable and desirable provisions for each of these roles and their corresponding stakeholders.

2. The prerequisite for criminalizing and punishing cyber threats and violations of cyber norms is the full dominance of "national" systems. But the "international" nature of the harm and dangers posed by these threats requires states to coordinate and synergize with one another, despite all the differences in domestic governance. Therefore, the realization of such a goal requires "respect" and "support" for both "national" sovereignty and the development of "transnational" interactions.

3. In order to institutionalize respect for and protection of national sovereignty in the common countering cybercrime, countries' "sovereign territories" and "nationalities" must first be recognized in the universal cyber landscape. In defining/drawing the territory of sovereignty, we should deploy all the opportunities and technologies provided in this space. For example, Country Code Top-Level Domain (e.g., .ir) can be a national symbol of a country, like its national flag. To identify nationals, an integrated global program must be developed and implemented to validate all individual electronic IDs.

4. In addition to determining "sovereign jurisdiction" in cyberspace on the basis of the determination of territory and nationality, the "enforcement capabilities" of national law must also be guaranteed and provided for Parties. Each system of government must be able to act on its own discretion to enforce its national law, especially, where transnational cybercrime has directly targeted their national order and security.

5. In addition to, or even more effective than, national government agencies, "e-service providers" are in various areas of infrastructure and application of information and communication technologies and play a decisive role against cybercrime. The type and extent of the responsibility of these global planners depend on the extent and variety of their cyber activities and services. The more impartial their activities and services are in terms of national issues –i.e., the more nations can use their services regardless of their national characteristics and circumstances–, the greater their duties and responsibilities are in preventing and responding to cyber threats. The point of interaction of the governing systems with this group of cyber activists are the "regulators" whose role and position should be assigned in different parts of the Convention.

6. This Convention focuses on the effective and efficient international combat against "cyber threats"; therefore, none of the issues related to Internet governance, cyber security, human rights standards, digital economy and its role in the sustainable development of countries and the like are central. However, all of them must establish their positive and negative role and position in this common international coalition to eliminate cyber threats from all global stakeholders. In particular, the laws and regulations governing each of these should not impose an inadequate ban or restriction on the implementation of global cybercrime programs.

7. The main priority in the universal criminal policy against cybercrime should be "prevention" of its occurrence, and the "response" to such crimes should be of paramount importance. The main reason behind this is that due to the advanced and sophisticated information and communication technologies available to cybercriminals, a significant portion of such crimes go undetected, and even those detected do not necessarily lead to the identification of the perpetrators; only a handful can be prosecuted. Common sense, therefore, dictates that cybercrime be prevented so that the international community can be protected from its devastating harm.

8. Achieving the three ultimate goals of deterrence, appropriateness and effectiveness of the universal cybercrime policy system, both in terms of preventive measures and response to cybercrime, requires the "comprehensive cooperation" of the involved Parties and communities. Therefore, in the first step, all countries must commit to establishing a great convergence and coordination at the national level between all governmental and non-governmental players, and be fully prepared to engage comprehensively with all competent transnational players. Identifying the role and position of each of the relevant governmental and non-governmental authorities and the type, level and extent of their transnational interaction can play an important role in achieving the objectives of the Convention.

9. The complex and continuously innovative technological nature of cyberspace has prevented most countries from experiencing an equal chance in the development and expansion of their infrastructure and applications. A group of countries referred to as "technology owners" have far more authority and initiative than the so-called "technology users". Therefore, in the joint combat against cybercrime, the security of the user countries,

even with the aim of protecting the countries with technology, should be a priority in the programs of the Convention.

10. The complex and continuously innovative technological nature of cyberspace prevents the reliable and inviolable implementation of the final document, at least for a short period of time. And at any time, an innovative technology or technological innovation may suspend a part of the substantive or procedural measures of the Convention. Therefore, establishing the "future research mechanisms" and even the "futurology" of universal cybercrime policy, along with the mechanism of immediate amendment of the Convention in order to prevent interruptions in transnational legal-judicial interactions, can significantly address the concerns arising from this undeniable feature of cyberspace.

11. Regarding the above-mentioned principles, it is worthwhile to take these following main subjects into consideration in the chapter of General Provisions:

    Article 1- The Convention’s objectives
    Article 2- The Convention’s scope
    Article 3- Definition of key terms