Andisheh Varzaneh Fanavari Tanzimi (Leinotech)
Islamic Republic of IRAN - Private Sector

Contribution on International Cooperation, Preventive Measures, and Technical and Training Assistance for the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

July 2022

I. International Cooperation

1. It is an undeniable fact that cybercrime has become a transnational phenomenon. This is what almost all Parties agree upon. Therefore, talking about international cooperation in countering cybercrime has become one of the evident necessities of the international cybercriminal justice system.
2. In addition to the above principle, the concern of Parties, especially "technology user" countries, should not be ignored; their sovereign system and their sovereignty over their territory and citizens have been adversely affected due to the interference of other sovereign systems, especially "technology owner" countries. This interference has excessively increased in their domestic affairs through ICT. In some cases, their sovereignty has been overshadowed by their measures and preparations in the transnational combat with cybercrime. Therefore, international cooperation should aim at reviving and re-establishing domestic legal systems in criminal governance over transnational cybercrime and minimizing the intentional or unintentional interventions of other governing systems.
3. Given the facts above, the most significant principles that have to be considered in the development of legal cooperation in combating cybercrime are (a) maximum national de-obstruction; (b) maximum transnational interoperability; (c) maximum assistance; and (d) maximum compliance.
4. Based on the above principles, the most important objectives that can be expected to be achieved from the development of legal cooperation in combating cybercrime are (a) increasing the cost of cybercrime; (b) preventing the displacement of cybercrime; (c) maximizing compensation for harm and damages caused by cybercrime; (d) preventing the repetition of cybercrime; (e) minimizing the cost of preventing and prosecuting cybercrime; (f) rehabilitating cybercriminals; (g) protecting the fundamental rights of individuals as well as national sovereign system; and (h) improving the level of legal and judicial insight and knowledge of beneficiaries and relevant cybercrime authorities.
5. In identifying the barriers to the development of international cooperation in combating cybercrime, the most important legal impediment is decriminalization and, at the same time, making offence of reprehensible cyber conducts (and needless to say, abandoning them). With the emergence and expansion of regulators in various sectors related to cyberspace, the list of crimes and the type and the number of criminal sanctions have gradually decreased, but the list of offences and regulatory sanctions have increased. This has caused Parties to have grave doubts about the development of their transnational legal cooperation. Therefore, with the

development of cooperation of the regulators to offences, the existing obstacle to combating these conduct that violate the norms of cyberspace may be reduced to some extent.

6. In addition to all this, despite all the achievements that the extremely easy interaction of the non-governmental sector and even citizens with governmental institutions and officials, and even the non-governmental sector and citizens of other Parties in various legal and judicial issues, can bring about, it may lead to the weakening of the system of national sovereign systems, and in practice marginalizing it. Therefore, the assessment and selection of an intermediary ground, in which not only the stability of national sovereign systems is secured, but the possibility of developing comprehensive transnational cyber legal and judicial relations between all beneficiaries is provided, is considered to be one of the innovative issues of international cyber law, especially criminal law.
7. Despite all the considerations that may affect the type and extent of transnational legal relations between Parties, undue discrimination must be avoided as much as possible, so that the field of cyber-international legal cooperation could reflect a reasonable balance between the Parties of the Convention, and that all Parties could have a tangible understanding of the fact that they could count on the legal cooperation of other Parties and would not be subject to unjust and illegal sanctions and restrictions by other Parties and countries.
8. In addition to observing the above principles and objectives, in order to operational effectiveness on cybercrime cooperation, there must be the possibility of both voluntary and request-based cooperation for all Parties, whether or not they have jurisdiction, so they could be given the opportunity to provide data and information that would help better advance the prevention and combating cybercrime.
9. Given the technology-oriented nature of the Convention, it is appropriate for members to boost their confidence in new technologies, especially convergent technologies, and by means of prioritizing their use in the development of their cybercriminal legal relations, they could operationalize new technologies application in the various stages and sections of the above cooperation by the needs analysis. Creating a national single window, shared cloud computing, simultaneous record of transactions on Distributed Ledger Technology (DLT), and joint big data analysis based on artificial intelligence, are the most prominent options that can be considered by members to combat cybercrime as effectively and efficiently as possible.
10. Physical and digital recovery of the material, moral and digital assets of cybercrime, including the tools and wares used in the crimes and their illicit proceeds, is one of the deadliest blows to the body of international cyber criminals. To achieve this, it is necessary to establish the highest level of coordination and cooperation between the competent judicial, executive, financial, and credit authorities of Parties and take advantage of all the available opportunities and capabilities to deprive cybercriminals of their criminal proceeds and compensate for the damages as much as possible.
11. In order to uphold the principle of sovereignty, Parties adhere to the principles of data and information processing, and other than the channels and mechanisms outlined in the Convention and mutual cooperation treaties –which shall not contradict with the provisions of the Convention– not to deploy other mechanisms for obtaining and receiving electronic evidence and always adhere to the principle of non-illegally obtaining of evidence. Parties may not disclose administrative correspondence and reported, educational and research data and information to an incompetent third Party or international authorities without the explicit and prior consent of the providing Party, or disclose it publicly and in violation of the rules established between the two Parties. Therefore, the regulation of the Convention need to be

done in such a way that it is possible for the harmed Parties to be compensated for the violation of these obligations.

12. At last, the establishment of joint physical and virtual research teams between Parties can lead to the maximum transnational de-obstruction, interaction, assistance, and compliance, so that Parties could arrange their multilateral cooperation more expeditiously, accurately and effectively, away from the time-consuming formalities of mutual cooperation.

II. Preventive Measures

1. Prevention is any measure that in the first step prevents the "emergence" of the elements that constitute a crime and in the next step prevents these elements from forming "bonds" with each other.
2. Thus, if the level of awareness of individuals about crimes can be raised, either in general or in particular (according to the circumstances and characteristics of each of them), it can be hoped that an important step in Crime prevention will be taken. This is because potential criminals, aware of the consequences of committing a crime, will avoid the emergence and development of criminal motives in their "essence", and victims, cognizant of the [peculiarities of the] crimes involving them, will act more cautiously, and while avoiding the provision of the necessary causes and elements of the crime, they take necessary precautions against the “targets”. The set of measures that lead to the growth of "awareness", both in potential offenders and in potential victims, is called "social prevention".
3. On the other hand, the set of measures taken by potential victims, other stakeholders, and relevant legal authorities to eliminate crime opportunities and technologies falls under the topic of "situational prevention". Here, the goal is to free the public, dedicated, and private ecosystems of potential victims from the causes, factors, and elements that create and nurture criminal opportunities and technologies. Therefore, in this field, as much as the actors themselves (both criminals and victims) require due attention, and perhaps even more, their ecosystems, conditions, and characteristics need to be attended to.
4. It is acknowledged that for a variety of reasons, preventing "cyber" crimes is far more difficult than "traditional" crimes. The main reasons and factors that make cybercrime prevention unsuccessful are:
    a. Misunderstanding of the reality of cyberspace and its criminal threats;
    b. Low level of cyber knowledge and insight;
    c. Cybercriminal easy networking;
    d. Easy victim identification;
    e. Anonymity;
    f. Accessibility of advanced cyber technologies for criminals;
    g. The internationalism of the cyber-world;
    h. Lack or absence of communication infrastructure and applications, information technology, and interactive data;
    i. Lack of cooperation and synergy of cybercrime prevention programs;
    j. Diminishing the Role of Governments in the Prevention of Cybercrime;
    k. Presence of third parties in the management and monitoring of the cyber-world;
    l. Lack of availability of new and up-to-date preventive technologies;
    m. Not having similar perspectives on cybercrime threats;
    n. The aggressiveness of cyber-prevention.

5. Despite all these issues, prevention is undeniable and inevitable and must be planned and implemented in such a way that the flaws and shortcomings as well as the challenges and tensions arising from it are eliminated or minimized. Therefore, the requirements of cybercrime prevention can be considered as follows:
   a. Prevention of all types of violations, including crime, offence, deviation/infringement, and harm; (From the prevention viewpoint, there is no difference between the above behaviors, and only the amount of material and moral damage is the criterion for their classification. Therefore, all these violations are reprehensible and harmful and should be prevented. It is worth mentioning that they have meaningful connections, and many of them are known to be more evolved and, of course, more dangerous than their simpler examples).
   b. Production and distribution of awareness-raising and general training content for common and current cyber threats (digital literacy promotion); (the main cause of vulnerability of users in this environment is due to their lack of awareness or fallacious awareness of the above threats).
   c. Production and distribution of specialized training and test content for users of specialized cyberspace fields and branches on threats and up-to-date prevention and countermeasure strategies; (Content testing means that the user in the relevant fields and branches, is subject to passing the awareness test).
   d. Special planning for the awareness-raising and distinctive education of users at risk, especially children and the disabled, for easy learning and preparedness in the face of threats;
   e. Adherence of agents in various sectors of cyber services to the implementation of the rules and requirements of the professional codes of conduct and ethic charters;
   f. Effective supervision of binding documents of cyber services, including various regulations, contracts, and policies such as safeguarding privacy and user rights;
   g. Organizing digital identity and regulating cyber anonymity mechanisms;
   h. Promoting and developing self-regulatory and self-control mechanisms for services and operators in various sectors of cyberspace, such as platforms, networks, and social media;
   i. Establishment of 24*7 cyber observation, monitoring, surveillance, and filtering centers at various public, specialized and technical levels that can be implemented by competent governmental institutions and qualified non-governmental sectors;
   j. Prioritizing cyber threats based on indicators such as vitality, sensitivity, and importance; or the extent of damage or loss resulting from their occurrence; or the number of potential victims; or the difficulty of dealing with intimidators in the event of fulfilling their criminal intentions, in order to maximize and optimally allocate funds for preventing them.
   k. Availability and affordability of efficient and effective hardware and software systems in preventing cybercrime threats for potential victims, especially those who are unable to provide them and at the same time who are vulnerable to threats;
   l. Developing cooperation and synergy protocols for the sharing of data and information and the interoperability of networks and communication systems and information technology between vulnerable countries or companies in the face of common threats;
   m. Elimination of unnecessary administrative formalities; and organizational and structural agility of governmental, non-governmental, and social mechanisms involved in cybercrime prevention programs;
   n. Increasing the cost of crime for those who, for unjustified reasons, refuse to adhere to and implement cybercrime prevention measures.

6. The formation of specialized committee for "Cybercrime Prevention" is proposed. Regarding this Committee, the main focus is on the types of preventive measures that can be taken against cybercrime, which generally fall into two above-mentioned categories: situational and social preventive measures. An independent branch is also proposed to be dedicated to legal and judicial prevention to continuously monitor the provisions of the Convention, and more importantly to review and analyze the substantive and procedural laws of Parties, especially those that play a decisive and effective role in the main and current processes of international cybercrime. And while identifying the obstacles and limitations arising from them, corrective approaches may be proposed to the authorities of the Convention and the relevant Parties.

III. Technical and Training Assistance

1. One of the main prerequisites or preconditions for the implementation of the Convention is for Parties to be more persevering in assisting each other to empower and prepare as much as possible to participate in international cybercrime policy. Undoubtedly, “countries with technology” have a momentous responsibility here, and they help the "countries using technology", and while removing the obstacles and limitations before them, “the countries with technology” provide the necessary opportunities for the proper exploitation, and empower and assist “the countries using technology” with various aspects, especially technical ones.
2. However, if the assistance of the Parties to each other, especially within the framework of the objectives and provisions of the Convention, is not systematized and regulated, which may inflict harm or damage on Parties, both the providing and receiving. This gradually undermines the achievements of the Convention and becomes a criminal threat.
3. Despite the maximum approach to the provision of assistance, the Convention provides conditions for the types of assistance, as well as for the providing and receiving Parties to maintain the independence of Parties and the effectiveness of assistance, so in the meantime and by providing assistance, no further damage or abuse could emerge, exacerbating the harm caused by cybercrime.
4. The formation of specialized committee for "Technical and Training Assistance" is proposed. Regarding this Committee, the main focus is on the types of assistance and the conditions for granting and benefiting from it. The goal is to achieve the highest level of productivity and to get as much assistance as possible to those Parties who are more eligible based on the expressed and verified criteria, and in turn, assisting them, especially with a transnational and international perspective, as this eliminates more harmful and widespread criminal threats. In addition, the application of monitoring and auditing mechanisms prevents possible abuses by either of the Parties and ensures the transparency and soundness of the assistance processes within the framework of the Convention.