United Nations A/AC.291/4

General Assembly

Distr.: General
17 November 2021
English
Original: Arabic/Chinese/English/
Spanish

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Compilation of views submitted by Member States on the scope, objectives and structure (elements) of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

Note by the Secretariat

Summary

In preparation for the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, the present note was prepared by the Secretariat pursuant to the instructions of the Committee Chair. It contains the views received from Member States on the scope, objectives and structure (elements) of the new convention.

V.21-08420 (E) 101221 131221

Contents

I. Introduction

1. In preparation for the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, on 11 August 2021 the Chair of the Committee, Ms. Faouzia Boumaiza Mebarki (Algeria), invited Member States to submit their views on the scope, objectives and structure (elements) of the new convention. The deadline set for submitting these views was 29 October 2021, subsequently extended to 5 November 2021.

2. The Chair also instructed the secretariat to compile the views as received and to translate them into the six official languages of the United Nations, to be made available for the first session of the Ad Hoc Committee.

3. The present note was prepared by the secretariat pursuant to the instructions of the Chair and contains the views received from Member States on the scope, objectives and structure (elements) of the new convention.

II. Views received from Member States

Australia

[Original: English]
[29 October 2021]

Australia welcomes the opportunity to submit its views on the scope, structure, and objectives of a new international convention on cybercrime. The new convention offers an unrivalled opportunity to secure widespread consensus on international cooperation to counter cybercrime, enabling States to better combat this pervasive and constantly evolving threat.

A new convention will only be valuable if it can secure widespread support among the majority of Member States, based on consensus agreement obtained from good faith discussions under the auspices of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established pursuant to General Assembly resolutions 74/247 and 75/282. To this end, Australia is committed to an open, inclusive, transparent and multi-stakeholder process, which offers the best chance of ensuring that States can arrive at an outcome acceptable to the largest possible number of States. This is in line with the principles set out in the past submissions by Australia to the Ad Hoc Committee, as well as the joint submissions in which Australia has taken part. Australia takes this opportunity to reiterate the points made in those submissions.

Cybercrime threatens all States, but it poses particular challenges for small States. Effective international cooperation on cybercrime is especially important for small island developing States, to help enhance their domestic capacity to combat transnational cybercrime operations. It is imperative that small island developing States are able to engage meaningfully in the work of the Ad Hoc Committee. Australia is committed to ensuring that there are adequate opportunities for Pacific island countries to participate in the work of the Ad Hoc Committee. Australia welcomes the decision to support hybrid (in person and online) participation in the sessions of the Ad Hoc Committee and emphasizes the importance of ensuring adequate preparation and participation time for smaller delegations.

Private sector entities play a unique and invaluable role in addressing cybercrime. To succeed, the work of the Ad Hoc Committee must therefore take account of the valuable expertise provided by industry stakeholders. States should also be responsive to the vast insight and expertise that other non-State actors, such as civil society organizations, academics and intergovernmental bodies, can contribute to the discussion on how best to combat cybercrime. To ensure

well-informed discussions and effective outcomes, the Ad Hoc Committee should afford these groups as many opportunities as possible to contribute.

Scope

Given the short time frame for negotiations, States have limited time to reach agreement on the many issues that comprise a new convention. The scope of the convention must be clearly defined and should focus closely on the criminal justice response to cybercrime. It should not address broader cybersecurity issues that are addressed in other forums.

To accelerate our work, States should focus their attention on areas where common approaches to cybercrime are needed. The work of the Ad Hoc Committee should adopt concepts and terminology related to cybercrime and international cooperation on criminal justice that are already well understood by the international community. We do not need to "reinvent the wheel", nor do we wish to create ambiguity.

The new convention should therefore draw heavily from the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption, as well as from other concepts that have been agreed by consensus at United Nations congresses on crime prevention and criminal justice and in other United Nations forums, as appropriate. It should be informed by effective existing international instruments that States have already adopted at the international and regional levels, such as the Council of Europe Convention on Cybercrime, and must avoid undermining existing norms established in those agreements. This is in line with the mandate contained in General Assembly resolution 74/247, in which the Assembly called for the work of the Ad Hoc Committee to take into full consideration existing international instruments and efforts at the national, regional and international levels.

In particular, the convention should continue to use the term "cybercrime". This term reflects a widely understood concept and has been used in countless United Nations documents, including the outcome documents of the Twelfth, Thirteenth and Fourteenth United Nations Congresses on Crime Prevention and Criminal Justice, as well as in General Assembly resolutions (most notably resolution 65/230) and many other resolutions and reports of the Commission on Crime Prevention and Criminal Justice and the Economic and Social Council.

Treaty elements (structure and objectives)

Criminalization

The new convention offers the opportunity to substantially improve international cooperation in relation to cybercrime. Harmonized standards for a core set of cybercrime offences will increase the ability of States to respond to cybercrime at the global, regional and domestic levels.

To this end, Australia considers that the convention should take a focused approach to the types of criminal conduct that have been substantially altered by cybercrime. The domestic criminal laws of States are typically more than adequate to define familiar crimes such as trespass, vandalism, theft, narcotics-related crimes and violent crimes. The convention does not need to reimagine these crimes simply because a computer or information system was involved in their commission.

The new convention must include new standards for criminalization of offences that can only be committed through the use of information and communications systems, known variously as "pure cybercrime" or "cyber-dependent crime". Such crimes did not exist before the advent of information and communications networks, and the domestic criminal laws of States are often insufficient or inconsistent in their applicability to such crimes. In this realm, harmonized standards for criminalization will offer considerable benefits for States, both in terms of their own domestic efforts to combat cybercrime and in facilitating greater international cooperation.

Similarly, Australia considers that there are some “traditional” crimes whose scope, scale and ease of commission have all been drastically increased by the speed, anonymity and widespread reach that information and communications networks provide. These are sometimes described as “cyber-enabled” crimes. The convention should address these crimes judiciously, by developing a clear framework for identifying why certain crimes are so significantly altered by a “cyber” element as to require a new harmonized international standard that elevates such conduct above “traditional” crimes. The Convention does not need to create new categories of offences for every existing crime that may incorporate a “cyber” element, particularly where the severity or scope of the criminalized conduct is not significantly altered by that element.

Australia considers that there are two obvious candidates for the category of cyber-enabled crimes that should be included in the convention: the severe threat posed by child sexual exploitation and abuse online, and the widespread and significant increase in cyber-enabled fraud and theft, including ransomware-related extortion. Australia is open to hearing arguments in support of other cyber-enabled crimes, but, for the reasons outlined above, the convention should adopt a restrained approach to including any new crime category.

The convention should also give due consideration to predicate offences and ancillary liability for cyber-dependent and cyber-enabled crimes. This should include the standard extensions of criminal liability included in instruments such as the Organized Crime Convention and the Convention against Corruption. Given the role of technology in facilitating cybercrime, the convention should also consider a harmonized criminal standard for offences involving the production, procurement or provision of technology and software adapted solely or primarily for the commission of cybercrimes.

Cybercrime is a rapidly evolving area, and cybercriminals consistently seek to deploy new technologies and methodologies to expand their activities and evade law enforcement. To counter this, the convention must ensure that criminalization standards are drafted in a technologically and methodologically neutral fashion, to ensure that the treaty remains relevant and effective into the future.

Procedural measures to combat cybercrime

Procedural law is a critical element of investigating and prosecuting cybercrime. The convention should provide a clear framework of procedural measures to ensure that law enforcement authorities can obtain the evidence needed to combat cybercrime. The scope of any framework of procedural measures should support clear domestic laws that are robust enough to allow for law enforcement or other relevant authorities to combat the challenges of cybercrime, including through detection, disruption, prevention, investigation and prosecution.

Procedural measures should also account for the nature of electronic data, ensuring that law enforcement and other relevant authorities can obtain such data quickly and effectively to ensure that criminal methodologies and practices in cyberspace do not disrupt authorities’ collection efforts. The types of procedural measures provided for could include search and seizure powers, powers related to the production of data (such as access to stored communications and interception activities), and emergency or urgent requests or orders for the disclosure of such data. Procedural measures must be underpinned by robust safeguards and limitations that adequately protect human rights and the rule of law.

States will likely need to consider how State practice relating to the collection of electronic data across jurisdictions will be captured in a new convention.

International cooperation and technical assistance

Cybercrime is overwhelmingly transnational in nature. International cooperation, supported by harmonized criminalization, is crucial to the ability of States to effectively investigate and prosecute cybercriminals.

The international community has made significant progress on international cooperation on criminal justice in the past decades, developing effective tools across a range of existing international treaties governing mutual legal assistance, extradition and other forms of international cooperation. The provisions of the Organized Crime Convention and the Convention against Corruption, for example, provide an excellent basis for such cooperation, and have been almost universally adopted.

The new convention should draw as much as possible from similar provisions of the Organized Crime Convention and the Convention against Corruption relating to mutual legal assistance, extradition, the transfer of prisoners and the recovery of proceeds of crime. These provisions have proved effective and enjoy broad international support. In line with the mandate contained in General Assembly resolution 74/247, it should also be ensured that the new convention complements and does not undermine other existing mechanisms for international cooperation on criminal justice.

Other international and regional regimes provide effective frameworks for international cooperation to counter cybercrime, underpinned by robust safeguards and limitations. The new convention should draw from these regimes as much as possible. Chief among them is the Council of Europe Convention on Cybercrime, which continues to provide an effective basis for international cooperation among a large number of States in all regions of the world.

In addition to international cooperation, the new convention should provide a meaningful boost to efforts to improve international capacity to combat cybercrime. The language should reaffirm the principal role of the United Nations Office on Drugs and Crime in providing technical assistance and capacity-building, including as the convenor of the Global Programme on Cybercrime.

Safeguards to protect and promote human rights

State access to the electronic and telecommunications data of individuals, by its very nature, has an impact on individual rights. The convention must reaffirm the responsibility of States to promote and protect the human rights of individuals in the States' efforts to combat cybercrime, consistent with international human rights law.

The rights of individuals to privacy and to freedom of opinion, expression and association must all continue to be adequately protected, in line with existing international standards. Other rights that must also be protected include the right to a fair trial, including equality before the law, as well as the right to freedom from torture and inhuman or degrading treatment or punishment, arbitrary detention and discrimination. The international community has repeatedly reaffirmed that these rights apply online just as they do offline, and the convention should reiterate the existing responsibilities of States to uphold these rights in the course of their counter-cybercrime operations.

Structure and method of work

Once States have had the opportunity to express their views in relation to the scope of the convention at the first negotiating session, to be held in January 2022, Australia anticipates that a consensus on the structure for the convention will emerge quickly.

After States have expressed their views as to the scope, structure and objectives of the new convention in January 2022, Australia proposes that States be invited to submit proposals on clauses to be included under each structural element of the new convention (for example, proposals on criminalization and international cooperation).

The Chair, in consultation with the Bureau as necessary, should then work to synthesize these various proposals into a draft, which States could then negotiate, with each set of clauses to be considered in turn according to a workplan established by the Ad Hoc Committee at its first meeting.

Following initial negotiations on each element of the structure, the convention could be further negotiated as a whole, again according to a workplan established by the Ad Hoc Committee at its first meeting and managed by the Chair thereafter.

Brazil

[Original: English]
[29 October 2021]

As in the case of many countries, Brazil has been dealing with cybercrime, a phenomenon that is increasing in frequency and sophistication. The migration of various criminal offences to digital platforms demands decisive efforts towards updating the proper normative and law enforcement response to the threats, including internationally. Their geographical extent and operational speed challenge traditional mechanisms of law enforcement and legal cooperation worldwide.

The challenges are tremendous. Internet service providers, which hold important information needed to investigate cybercrime and collect electronic evidence, frequently have physical headquarters in one country, provide services in different continents and store their information on servers anywhere else on the planet. In this scenario, law enforcement authorities strive to identify and duly address whoever has jurisdiction over and direct access to the data.

The cohesive international coordination of jurisdictions is a necessary step forward in prosecuting cybercrime. More and better cooperation is needed. Effective disruption requires agile and direct means of cooperation by which law enforcement agencies can share evidence from different cases involving the same criminal group in a timely fashion.

Brazil is fully engaged in the negotiation of a comprehensive convention on countering the use of information and communications technologies for criminal purposes. It is a singular opportunity to establish common standards for cooperation in tackling such an essentially transnational issue, building on the best traditions and practices in that regard.

From the perspective of Brazil, a future convention, in order to be capable of responding to the aforementioned challenges, must address the following elements in terms of objectives, scope and structure.

Objectives

The main objective of the convention should be to provide specific tools for international cooperation, so that States parties have timely access to evidence and other information that contributes to the investigation and prosecution of cybercrime. In spite of the merit that this primary objective enjoys autonomously, the instrument should, ideally, also contemplate two other objectives: (a) the establishment of minimum criminalization obligations (substantive criminal law) in each jurisdiction of the States parties; and (b) the establishment of minimum obligations to enable timely response, investigation and prosecution (procedural criminal law) in each jurisdiction of the States parties.

Brazil is fully committed to the idea of a universal convention. We are sensitive to the challenges of negotiating an instrument that contains minimum standards of criminalization, particularly in view of such a modern and volatile phenomenon. There are successful precedents in this direction, however. In other criminal areas, such as the existing universal crime conventions, effective negotiations have allowed most of the world to commit to minimum substantive standards. The debate should

not start from a presupposed antithesis between geographic scope and the scope of criminalization, but rather from the understanding that the negotiations themselves will be the safest method to obtain the best measure of the minimum possible consensus on substantive criminal law on cybercrime. As restricted as it may be, a minimum consensus on criminalization – well founded on neutral and generic concepts – could limit cybercriminals' choice of jurisdiction, facilitate the exchange of experiences and reduce normative dissension between countries that demand application of the dual criminality principle to cooperate.

The timeliness of international cooperation will always depend on the procedural instruments available to investigators, prosecutors and judges in the most diverse jurisdictions. Nowhere are traditional instruments of legal cooperation, such as the letter rogatory and the recognition of foreign judgments, able, by themselves, to assure an adequate reaction to cybercrime. The transnationality and extreme volatility inherent in the phenomenon demand procedural standardization, even if it is as flexible and generic as necessary to contemplate all the specificities of the domestic legal systems involved. The core of this procedural standardization, however, should address some minimum standards in order to enable the expeditious preservation of electronic evidence, activated by an agile and direct international channel, otherwise it will not allow the identification of criminals, especially in cases of organized crime.

Scope

The convention should provide a basis for the exchange of evidence and data relating to: (a) crimes against computer systems; and (b) any crimes that are committed by electronic means. Ideally, electronic data related to connections, content and subscribers should be addressed.

The convention should also allow parties to make requests for international cooperation (for expedited preservation of electronic data and for mutual legal assistance) and to transmit spontaneous information to other jurisdictions. A chapter would have to be dedicated to building an international network of practitioners who would be responsible for responding to urgent cases. Such an operational mechanism reinforces the understanding that such a convention requires establishing a decision-making body for monitoring and reviewing its implementation.

As a framework instrument, the treaty could establish the possibility of negotiating protocols as additional tools, which would deepen cooperation on specific cybercrime typologies.

The convention should therefore constitute an instrument for the practical application of criminal law, not delving into policy on international peace and security, cyberdefence or issues relating to the structure or governance of the Internet at the domestic, regional or global levels.

Structure

In the light of the aforementioned considerations, Brazil deems that the convention should have the following structure:

Chapter I. Criminalization

Chapter II. Criminal procedural law enabling timely investigation and prosecution

Chapter III. International cooperation

A. Expedited preservation of electronic data

B. Mutual legal assistance

C Spontaneous information

Chapter IV. Cooperation network

Chapter V. Follow-up mechanism for monitoring and reviewing implementation

Canada

[Original: English]
[1 November 2021]

The present submission by Canada is in response to the invitation by the secretariat of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes of 11 August requesting Member States to submit views on the scope, objectives and structure (elements) of the new convention.

In preparing these comments, Canada is inspired by the important work that has been done within the United Nations on cybercrime over more than 20 years under the auspices of the Commission on Crime Prevention and Criminal Justice, in particular by the intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, the United Nations Drugs and Crime Office, through its Global Programme on Cybercrime, and the United Nations congresses on crime prevention and criminal justice. These initiatives have set the stage for the elaboration of a United Nations convention that should exclusively focus on the fight against cybercrime and not deal with cybersecurity, cybergovernance and other related matters better addressed in other United Nations forums.

In accordance with General Assembly resolution 75/282 and its past submissions to the Ad Hoc Committee, Canada would like to reiterate that the negotiation of the new convention must be a transparent and inclusive process, allowing civil society and other relevant stakeholders a meaningful opportunity to participate.

Scope

The new convention should provide a framework to counter cybercrime and serious criminal offences that are frequently committed through the use of computer systems that includes the following elements:

(a) Provisions for substantive cybercrime offences and the investigation and prosecution of cybercrime and serious criminal offences that are frequently committed through the use of computer systems;

(b) Provisions for international cooperation in relation to the above, as well as for obtaining electronic evidence of other criminal offences;

(c) Provisions that include measures that seek to prevent cybercrime; and

(d) Provisions that include measures that encourage Member States and other stakeholders to provide sustained technical assistance and capacity-building initiatives.

The elements of the new convention must be consistent with international human rights obligations, in particular in relation to the freedoms of expression, opinion and association, as well as the right not to be subjected to unlawful or arbitrary interference with one’s privacy.

Objectives

The new convention should have the following objectives:

(a) On the basis of a common understanding, establish a baseline for substantive criminal offences, procedural powers and international cooperation to fight cybercrime;

(b) Ensure provisions are drafted in a technologically neutral way in order to ensure that the provisions do not become obsolete or unenforceable as technologies evolve;

(c) Promote and facilitate international cooperation in the common fight against cybercrime;

(d) Establish the authority to collect, obtain and share electronic evidence of other offences;

(e) Eliminate safe havens for cybercrime perpetrators;

(f) Ensure compliance with international human rights obligations, in particular in relation to the freedoms of expression, opinion and association, as well as the right not to be subjected to unlawful or arbitrary interference with privacy;

(g) Ensure consistency with existing United Nations treaties in the field of crime prevention and criminal justice, in particular the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption, and take into account multilateral instruments that have already proved their usefulness in the fight against cybercrime, in particular the Council of Europe Convention on Cybercrime; and

(h) Support Member States to strengthen their capacity to address cybercrime through technical assistance and capacity-building.

Structure

With regard to the structure of the new convention, and in addition to clear definitions and final provisions, Canada considers it important that the following five elements form part of the structure of the convention:

(a) Substantive offence provisions requiring Member States to adopt legislative and other measures as may be necessary:

(i) To establish as criminal offences actions affecting the confidentiality, integrity and availability of computer systems, networks and computer data, and the misuse of computer systems, networks and computer data; and

(ii) To ensure that specified traditional crimes frequently committed through the use of computer systems are adequately covered by their criminal law, for example, the dissemination of child pornography;

(b) Procedural provisions requiring Member States to adopt legislative and other measures as may be necessary to establish the authority to preserve and obtain electronic evidence of criminal offences that is stored on computer systems in foreign, multiple or unknown jurisdictions. While more general investigative powers, such as search and seizure and production orders, should be included in the new convention, more specialized investigative tools should also be included to address the speed at which offences can be committed and the transience and volatility of electronic evidence. These provisions should be subject to safeguards to ensure that law enforcement activities comply with international human rights obligations;

(c) International cooperation is important in combating cybercrime. The new convention needs to include mechanisms to facilitate both formal and informal international cooperation for the detection, investigation and prosecution of cybercrime, as well for obtaining electronic evidence of other criminal offences;

(d) The new convention needs to include preventive measures similar to those set out in the Organized Crime Convention and the Convention against Corruption, for instance, provisions on awareness-raising and educational initiatives. Multi-stakeholder partnerships and civil society can play a vital role and this should be reflected in these provisions;

(e) The new convention should encourage Member States to strengthen capacity to address cybercrime through technical assistance and capacity-building. This could include provisions to:

(i) Support multi-stakeholder involvement;

(ii) Encourage collaboration with the United Nations Office on Drugs and Crime and its Global Programme on Cybercrime to enhance the skills of practitioners and central authorities in the use of technology to facilitate international cooperation in fighting cybercrime; and

(iii) Develop training programmes for investigators and prosecutors and support the sharing of information and experiences with relevant stakeholders.

Chile

[Original: English]
[5 November 2021]

The Government of Chile is pleased to respond to the invitation to Member States to submit their views on the scope, objectives, and structure (elements) of the new convention, with regard to the implementation of General Assembly resolutions 74/247 and 75/282.

Chile considers that the new convention should not conflict with other pre-existing treaties or agreements on cybercrime. It should be based on international cooperation and technical assistance as the foundation of the multilateral approach to the fight against cybercrime. The views of all countries must be considered of equal importance, so as to maintain an open, inclusive, transparent and multi-stakeholder process.

1. General aspects

(a) *Jurisdiction*. The new convention is an excellent opportunity to discuss this issue, which is the basis for many of the procedural tools that can be addressed;

(b) Ensure that the definitions are drafted in a comprehensive way, so as to ensure their relevance and applicability in the context of rapid technological transformation. Include definitions, such as for the different types of data.

2. Substantive criminal law

(a) *Inclusion of the crime of receiving computer data*. Although some countries have a restricted conception of this crime type, it seems appropriate to include an illegal act that pursues this type of conduct when the "goods" stolen correspond to computer data and whoever stores them knows or could not but know of the spurious origin of the same;

(b) From the point of view of authorship and participation, it seems appropriate to specifically address the collaboration provided by the recipient of the money or securities illegally stolen through computer fraud, since, taking into account the particularities and investigative challenges presented by this class of crimes in the vast majority of cases, it is pertinent to give special treatment to the prosecution of those people who, as a general rule, constitute the first link to be followed in the criminal chain, thus it is appropriate to increase, on the basis of their participation, their status as authors of the fraud, without prejudice to the possibility of offering a reduction of penalties in case they provide effective cooperation in the capture of the remaining computer criminals.

3. Rules of procedural law

(a) It is appropriate to discuss possible new ideas and working tools that authorities could use for detecting crimes that are being elaborated or are intended to be carried out on the Internet, and the most effective way to confront this type of crime;

(b) It seems appropriate to discuss the balance that must be struck between the necessary and due protection of citizens and personal data and the criminal investigation, since overprotection of this type of information could generate consequences in the development of investigative procedures that enable the correct and timely criminal prosecution of this type of crime, which benefits from the anonymity, transnationality and lack of traceability that this type of behaviour brings with it.

4. Chapter on international cooperation

(a) It is important to establish principles on mutual legal assistance in criminal matters;

(b) Countries should explore ways to help to ensure that information is exchanged among investigators and prosecutors dealing with cybercrime in a timely and secure manner;

(c) Countries should cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat cybercrime. Each country should adopt effective measures to establish channels of communication between their competent authorities, agencies and services to facilitate the secure and rapid exchange of information concerning all aspects of cybercrime;

(d) Consider the electronic transmission of mutual legal assistance as a valid and permanent form and not only in emergencies;

(e) Preservation and delivery of data;

(f) Analyse the positive contribution of 24/7 networks as an innovative contribution to international cooperation;

(g) Regulate emergencies;

(h) Countries should jointly identify the existence of the “digital gap” between countries, as some countries lack the capacity and capability to prevent, detect and combat cybercrime and are more vulnerable in the face of cybercrime challenges.

5. Special tools for international cooperation

(a) Delivery of data by Internet service providers and their relationship with States;

(b) Cross-border data access;

(c) Special investigation techniques: online undercover agents, joint investigation teams and joint investigations, among others.

6. Prevention

(a) Prevention of cybercrime requires participation by various stakeholders, including governments, law enforcement authorities, the private sector, international organizations, non-governmental organizations and academia;

(b) Promote victim-centred prevention strategies that deal with interpersonal cybercrimes;

(c) Countries should consider implementing mechanisms for cooperating with industry, including referrals to competent national authorities and the taking down of

harmful criminal material such as child sexual exploitation material and other abhorrent violent material.

7. Gender perspective in the context of a cybercrime convention

(a) Include a gender perspective in the implementation and evaluation of the impact of the provisions of the convention and account for a gender-sensitive analysis when it comes to the use of information and communications technology, in particular when referring to gender-specific issues related to cybercrime, to promote gender equality and the empowerment of women online and offline;

(b) Address cybercrime and prevent and combat violence against women and children.

China

[Original: Chinese]
[5 November 2021]

China welcomes the invitation from the Chair of the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes for Member States to submit their views on the scope, objectives and structure (elements) of the convention. Pursuant to General Assembly resolution 75/282, the Ad Hoc Committee is to submit a draft convention to the General Assembly at its seventy-eighth session. China looks forward to constructive discussions under the leadership of the Chair to arrive according to schedule at a new convention that is universal, authoritative and acceptable to all parties, so as to provide a legal framework for strengthening cooperation in combating cybercrime worldwide.

Member States have thus far been using relevant United Nations mechanisms to conduct in-depth discussions on combating cybercrime and have reached some agreed conclusions and recommendations. One Member State has also put forward a draft comprehensive convention, providing an important reference for negotiation of the convention. China welcomes the efforts of the Chair to encourage Member States to actively submit their views and draft proposals, while supporting the Chair's preparations for a zero draft of the convention on the basis of Member States' submissions so as to begin negotiating the text of the convention as soon as possible.

In order to support the work of the Chair and the Ad Hoc Committee, China has drafted the following views on the scope, objectives and structure (elements) of the convention and stands ready to engage in constructive negotiations with all parties.

I. Objectives

(a) To promote and strengthen measures to combat and prevent more efficiently and effectively the use of information and communication technologies (ICT) for criminal purposes, in pursuit of the vision of a shared future in the cyberspace community;

(b) To promote, facilitate and support international cooperation in preventing and combating the use of ICT for criminal purposes, bearing in mind the particularities of ICT and the need to combat related criminal activities. Such international cooperation may include coordinating criminalization standards among Member States, providing guidance for resolving jurisdictional conflicts and developing more targeted institutional arrangements in law enforcement cooperation, legal assistance, extradition and asset recovery;

(c) To strengthen cooperation in capacity-building and technical assistance and promote the exchange of information in this field in line with broader international cooperation needs and the interests of developing countries.

II. Scope of application

The convention should apply to the prevention, investigation and prosecution of the use of ICT for criminal purposes by individuals or criminal groups, as well as the blocking, freezing, seizure, confiscation and return of the proceeds of ICT-related crimes.

The use of ICT for criminal purposes should apply, as a minimum, to crimes perpetrated against ICT facilities, systems and data as well as crimes committed using ICT.

III. Structure (elements)

The convention could be divided into seven chapters: general provisions; prevention; criminalization and law enforcement; international cooperation; technical assistance and information exchange; implementation mechanism; and final provisions.

The following preliminary suggestions are made with regard to the elements of the respective chapters.

1. General provisions

In addition to the objectives and scope of application, the content below should also be included:

(a) *Protection of sovereignty*. The principle of sovereign equality enshrined in the Charter of the United Nations is the basic norm of contemporary international relations. Application of the principle of sovereignty to cyberspace is also widely supported by Member States. The convention should specify that States parties are to carry out their obligations under the convention in accordance with the principles of sovereign equality, territorial integrity and non-interference in the internal affairs of other States;

(b) *Terminology*. Definitions should be provided for key terms mentioned in the convention, e.g. electronic evidence, personal information, critical information infrastructure, cloud storage, network service provider, malware, botnet, harmful information and cyberattack.

2. Prevention

The importance of preventing the use of ICT for criminal purposes should be highlighted. The basic principle should be that of “putting prevention first, while simultaneously combating crime”. The responsibilities of Governments and the private sector in crime prevention should be clarified, and Governments should formulate targeted crime prevention measures while encouraging the participation of society and public-private cooperation. The following points should be included:

(a) Member States should be encouraged to designate specialized agencies for developing policies on the prevention of the use of ICT for criminal purposes and for conducting assessments on a regular basis. Member States should establish security protection for critical information infrastructure as well as security protection systems based on different network levels. Different information security technologies and management measures should be adopted for different network facilities so as to protect critical information infrastructure from being attacked by criminals or criminal groups. The crime prevention capacity of relevant government departments should be enhanced;

(b) Member States should enact or improve national legislation to clarify the responsibilities of the private sector, including network service providers, in preventing the use of ICT for criminal purposes. Those responsibilities should include, among others, security precautions (for example, formulating emergency plans for network security incidents, addressing system and hardware vulnerabilities, computer viruses, network attacks or network intrusion in a timely manner, and taking

measures in real time whenever the services of such providers are found possibly to be used for criminal activities) and log information retention (Governments should specify the content standard and duration of log information retention). When determining the responsibilities of network service providers, arrangements tailored to each level and consistent with the principle of proportionality should be made, taking full account of the differences in capabilities of network service providers of different sizes;

(c) Governments, the private sector and communities should be encouraged to engage in various forms of public-private cooperation. In particular, more efforts should be made to enhance public awareness of crime prevention.

3. Criminalization and law enforcement

Criminals and criminal groups are increasingly abusing ICT to commit crimes, giving rise to a dark "production chain" specializing in the development of ICT for criminal purposes and transactions involving such technologies and related data. The convention should provide a more flexible and forward-looking framework for coordinating criminalization, responding to the needs of current and future ICT development and the need to combat crime. The convention should also provide for the relevant mechanisms in terms of jurisdiction, law enforcement and electronic evidence:

(a) Member States should be requested to criminalize the intrusion into and destruction of ICT facilities, systems, data or critical information infrastructure. This could include illegal accessing of computer information systems, illegal interference with computer information systems, illegal acquisition of computer data, illegal interference with computer data and infringement of critical information infrastructure, among others;

(b) The convention might enumerate, as appropriate, the criminal activities that are perpetrated by using ICT and are broadly recognized by the international community, such as cyberextortion, cyberfraud, cyberpornography (especially child pornography), the use of ICT to infringe copyright and related rights, and the use of the Internet to incite or commit acts of terrorism or disseminate harmful information, among others;

(c) With regard to other crimes committed by using ICT, it should be emphasized that Member States may combat and prevent relevant crimes not listed in the convention, and they may engage in international cooperation in accordance with the convention, other international conventions and the applicable national legislation of Member States;

(d) In view of the increasing "industrialization" of crimes committed by using ICT, the dark "production chain" should be included in the scope of criminalization, together with tighter measures to suppress the abetting or preparation of such criminal acts, including the development, sale or dissemination of ICT or data for criminal purposes;

(e) With regard to the term "electronic evidence", the rules for identifying electronic evidence in criminal judicial procedures should be stipulated, including how to ascertain the authenticity, integrity, legitimacy and relevancy of electronic evidence;

(f) Member States could be requested to formulate or improve national legislation with a view to clarifying the obligations of the private sector, such as the obligation of network service providers to cooperate with law enforcement authorities in monitoring, investigating and combating crimes. Such obligations should include, among others, retaining log information, preserving data and evidence in accordance with unified content standards and durations, and cooperating with law enforcement authorities. When determining the obligations of network service providers, arrangements tailored to each level and consistent with the principle of proportionality should be made, taking full account of the differences in the

capabilities of network service providers of different sizes. If a network service provider fails to perform its relevant obligations, Member States should impose effective administrative and criminal penalties on it in accordance with their national legislation;

(g) Guidance should be provided for resolving jurisdictional conflicts. Given the particularities of cyberspace and ICT, standards on how to determine jurisdiction and avoid jurisdictional conflicts should be provided. Jurisdiction should be based on a "true and sufficient" link with the criminal activity in question, giving priority to the place where the consequences of the criminal activity occur, the place where the crime was committed and the place where the person or group that committed the crime is located. If it is difficult to formulate such standards, then exclusionary standards should be put forward; for example, a State should not be able to claim jurisdiction over an ICT-related case merely on the grounds that the data passed through that State. In cases of jurisdictional conflict, the jurisdiction should be determined through consultation in accordance with the principles of forum conveniens and the facilitation of asset recovery;

(h) Provisions on aiding or abetting the commission of a crime, preparation of a crime, attempted crime, crime committed by an entity, etc., should also be made.

4. International cooperation

The use of ICT for criminal purposes is highly transnational and is a shared challenge facing the international community. In addition, the anonymity and high-level intelligence of criminal activities and the instability and perishability of electronic evidence pose significant challenges to international cooperation mechanisms such as mutual legal assistance under the existing international legal framework. Member States should cooperate with each other to the greatest possible extent in combating and preventing the use of ICT for criminal purposes, by upholding the principle of reciprocity, actively exploring institutional innovation and proposing new mechanisms for more targeted international cooperation:

(a) Cross-border collection of electronic evidence is necessary for combating the use of ICT for criminal purposes, but Member States should respect the sovereignty of the State where the evidence is located. Member States should also abide by due process, respect the legitimate rights of individuals and entities, and should not employ any invasive or destructive technical investigative means in cross-border electronic evidence collection. States should not directly collect data housed by enterprises or individuals in foreign States or by using technical means that bypass network security protection measures if such means infringe the laws of that foreign State. Member States should explore new institutional arrangements for collecting electronic evidence from other States, such as electronic evidence authentication and video (or audio) evidence collection on the basis of mutual trust. Efforts should be made in such arrangements to provide unified and authoritative guidance for cross-border electronic evidence collection while balancing the different aims of respecting national sovereignty and combating crime;

(b) Member States should formulate mechanisms for rapid law enforcement cooperation. Member States could designate specific agencies for liaison purposes, thereby allowing for the rapid sharing of crime clues, provision of technical advice and other forms of law enforcement cooperation in case of special needs;

(c) In order to improve the efficiency of mutual legal assistance in criminal cases, Member States could establish a rapid liaison and response mechanism between competent authorities to ensure real-time communication when necessary. The transfer of legal documents and electronic evidence as part of cross-border evidence collection could be done online through technical means (such as electronic signatures) within the framework of national cross-border systems for managing data transmission security. Provision could also be made for mutual legal assistance in emergency cases, such as expedited preservation of electronic evidence, expedited disclosure after data preservation, etc.;

(d) Given the obligations – to be established in national legislation – of the private sector, including network service providers, to cooperate with law enforcement authorities in monitoring, detecting and combating criminal activities, Member States, especially those having advanced network resources, should further strengthen international cooperation. If ICT facilities, systems or networks owned by a network service provider in State A are used by a suspect in another State to commit a crime, then as long as State A also criminalizes the act in question, State A should, on its own initiative or at the request of the other State, require the relevant network service provider to avail itself of the technical and any other measures necessary to effectively respond to the criminal activity;

(e) Relevant measures should be strengthened to prevent and block the international transfer of the proceeds of crime and enhance international cooperation in asset recovery. Member States should abide by the principle of rapid and effective asset recovery and should not set any preconditions for asset recovery other than judicial procedures.

5. Technical assistance and information exchange

It is essential to provide technical assistance to developing countries and strengthen the exchange of information with them in order to effectively combat and prevent the use of ICT for criminal purposes:

(a) Technical assistance provided to developing countries should include:

(i) Training for law enforcement and judicial personnel;

(ii) Training for professional teams possessing both legal and technical expertise;

(iii) Building capacity in the area of collecting electronic evidence;

(iv) Providing relevant equipment and technology, as appropriate, to help developing countries to strengthen their capacity to combat crime;

(v) Encouraging international organizations such as the United Nations Office on Drugs and Crime, the private sector, experts and academics to participate in technical assistance and capacity-building efforts;

(b) Member States should be encouraged to share their experiences in the formulation and implementation of laws and policies, and to share data related to combating and preventing crime and crime trends.

6. Implementation mechanism

In order to promote implementation of the convention, a conference of the States parties and relevant expert groups or working groups, such as a working group on technical assistance and a working group on international cooperation, should be established. The meetings of such groups could also provide a platform for States parties to exchange experiences and promote cooperation.

7. Final provisions

No comments at this point.

Colombia

[Original: Spanish]
[5 November 2021]

In view of the adoption of General Assembly resolution 74/247, through which an open-ended ad hoc intergovernmental committee of experts was established to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, and in response

to the invitation of the Chair of the Ad Hoc Committee to the Member States to submit their views on the scope, objectives and structure that the future convention on cybercrime should have, we wish to submit the following preliminary comments of Colombia.

Scope

The new convention should focus on the objective of an international legal cooperation tool for the prevention, investigation, prosecution and punishment by national authorities of cybercrime offences, and address matters relating to electronic evidence. Discussions that do not focus on the legal problem of cybercrime and the management of electronic evidence should therefore be avoided.

Discussions on issues that may be politically sensitive and that do not relate directly to the substance of the convention to be negotiated should be avoided.

It is essential that the new convention take into account existing international legal frameworks and instruments, including the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and the Budapest Convention on Cybercrime, since the national legislation and practices of most States are aligned with or based on existing agreements; consequently, future standards must be compatible with those agreements. Furthermore, it should be ensured that the rules to be elaborated do not give rise to incompatibility with, or do not conflict with, other international obligations undertaken by States.

In that respect, the convention should have a complementary approach, that is, the negotiations should, in principle, take into consideration the work that the international community has already been carrying out for several years in countering cybercrime and not contradict the relevant international obligations undertaken by States. Advantage should therefore be taken of the potential and progress that the United Nations Convention against Transnational Organized Crime has brought with it in terms of established principles and judicial cooperation tools.

Current multilateral, regional and bilateral frameworks for mutual legal assistance should be taken into account in order to avoid potential conflicts in laws and regulations, to complement and apply existing international instruments and to avoid hindering their effective implementation. Thus, it should be recommended that thorough consideration be given not only to multilateral precedents, such as the United Nations Convention against Transnational Organized Crime and the Convention on Cybercrime, but also to bilateral and regional agreements, such as the Inter-American Convention on Mutual Assistance in Criminal Matters.

Specifically, the Convention on Cybercrime (Budapest, 2001) should be taken into account, as it covers concepts that have been discussed extensively and reflects 20 years of practical international experience. Failure to do so would entail the risk of embarking on a path that would erode the progress already made in countering cybercrime.

The process should also take into consideration the results of the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime within the framework of the United Nations, and should draw on the list of preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group.

We underscore the importance of elaborating the new convention in an inclusive and transparent manner and – to the extent possible – on the basis of consensus, as was done in the earlier United Nations processes to conclude the Organized Crime Convention and the Convention against Corruption, in order to help prevent future disputes.

Objective

The general objective of the convention should be the adoption of a framework for international judicial cooperation that provides comprehensively for prevention, investigation and prosecution in countering the use of information and communications technologies for criminal purposes – cybercrime – and addresses matters relating to electronic evidence.

Structure

- Key definitions and standardized technological concepts that will remain valid over time.
- Substantive provisions (criminal offences to be established in national legislation).

In this regard, the convention should criminalize a range of acts that affect computer systems and information.

It would be logical, in terms of both principles and methodology, to focus exclusively on "core" cybercrime offences: offences relating to unauthorized digital access to computer networks or systems through the offence of illegally accessing a computer system; cyberespionage, which encompasses all acts that violate the privacy of natural and legal persons through the interception or obtaining of data, communications, files or databases stored in computer systems or transmitted through communication networks, and includes the offences of intercepting computer data, breaching personal data and creating phishing sites with the aim of capturing personal data; and computer sabotage, which is aimed at disrupting, damaging, rendering unusable, immobilizing or interfering with computer systems, databases or data processing, transfer and transmission processes and which includes the offences of unlawfully disrupting a computer system or telecommunications network.

In addition, the instrument could cover a number of acts that, because they are committed by digital means, have a serious and far-reaching impact and are difficult to investigate; this would make the convention flexible enough to serve as a tool for combating illegal activities related to other offences:

- Dual criminality clause: this mechanism is important in facilitating mutual legal assistance regardless of whether the act giving rise to such assistance is punishable under the law of the requested State, thus ensuring, inter alia, that cybercriminals do not find safe havens in some countries in the absence of common standard legislation.
- Procedural provisions enabling effective legal cooperation: in this regard, it is imperative to step up international cooperation in the investigation of cybercrime offences, especially in relation to the management of digital evidence, the chain of custody, data retention and forensic analysis. The transmission and storage of data is an issue that requires urgent attention, as well as the definition of mechanisms that enable rapid communication and response between counterpart authorities in different States, through appropriate and secure digital channels.
- Aggravating circumstances applicable to acts that affect the legal right to protection of information and of data, such as acts relating to the capture of personal data on a large scale, violation of human rights or acts targeting critical infrastructure and essential services.
- International judicial cooperation: facilitate, broaden and expedite mutual legal assistance requests through digital channels, with appropriate safeguards, and through standard formats.
- Define special investigative mechanisms for the gathering of digital evidence, especially in relation to evidence stored in different jurisdictions.

- It is important that the Member States agree mechanisms that ensure an adequate level of protection of personal data in the course of the exchange of information through the international instrument, not only because of the importance that protection of personal data has assumed in the digital environment but also in order to avoid the possibility that the particular rules of each country might pose an obstacle to the effective exchange of information between States.
- Promotion of technical assistance, dissemination of knowledge and good practices relating to investigation, prosecution and punishment. In addition, in order to bridge the digital divide, it is essential that the convention cover capacity-building for law enforcement institutions and other national judicial authorities, especially with regard to education and training programmes as a form of prevention.
- Promote, through regional training schools, technical cooperation. Given the complexity and specificity of the investigation of crimes that are committed through digital means and that hinder effective investigation, it is necessary to provide specialized training to prosecutors and investigators in an organized and continuous manner and on the basis of predefined workplans setting out expected results.
- The promotion of strong, trust-based cooperation between the public and private sectors in the area of cybercrime is of the utmost importance, which is why it is essential to reach a common position on the issue and to facilitate the gathering of digital evidence by actors in the digital domain, including Internet service providers and communications companies.
- Promote and facilitate the access of authorities to collaborative platforms for capacity-building and information exchange and to analytical and contextual tools for cybercrime investigations.
- Provisions that facilitate access to timely information in emergency cases.
- Lastly, it is suggested that the convention provide for the establishment of a network of points of contact operating 24 hours a day, 7 days a week, to respond to requests for international legal cooperation in relation to cybercrime. In addition, the network could be complemented by a network of contacts for: (a) promoting the sharing of knowledge and experience with respect to cybercrime and related offences; (b) establishing and disseminating good practices; and (c) optimizing and streamlining international judicial cooperation.

Dominican Republic

[Original: Spanish]
[5 November 2021]

The Dominican Republic welcomes the opportunity to contribute to this collective exercise with all Member States with a view to submitting comments on the scope, objectives and structure of a new international instrument on cybercrime, in accordance with General Assembly resolutions 74/247 and 75/282, of 27 December 2019 and 26 May 2021, respectively.

Cybercrime is an emerging form of transnational crime and one of the fastest-growing worldwide. Its rise is closely linked to the evolution and exponential development of information and communications technologies, affecting millions of citizens and businesses every year.

Our region, Latin America and the Caribbean, has been particularly affected by this phenomenon. Developing countries largely lack the capacity needed in order to combat cybercrime, a situation that has a direct impact in terms of the high number of persons recorded as having been victims of such crime.

Moreover, the recent coronavirus disease (COVID-19) pandemic has highlighted the vulnerability of the international community to cybercrime, a situation that has underscored the importance of a global response founded on collaboration and coordination, not only among Member States but also between Governments and non-governmental organizations, civil society, academia and the private sector, since the complexity and scale of cybercrime are such that any response must be based on a multidisciplinary approach if it is to be effective.

The Dominican Republic fully supports this endeavour on the part of the international community and reiterates its willingness to work together with all Member States towards the conclusion of an international treaty that represents each and every one of us, guided at all times by the principles of transparency, impartiality and inclusion.

Scope

The Dominican Republic is of the view that the primary purpose of a new international instrument on cybercrime is to provide an effective tool for the prevention, detection, investigation and criminal prosecution of cybercrime, with full respect for privacy, data protection, civil liberties and human rights.

In particular, the instrument should facilitate criminal investigation processes, enabling the timely collection and subsequent use of digital evidence and thus reducing impunity for this type of crime, such impunity being one of the main constraints faced by law enforcement officers in the field.

It should also promote and facilitate international cooperation among Member States and technical assistance and capacity-building in States parties that require such support in relation to cybercrime.

The Dominican Republic is also of the view that it should be clearly established that the new instrument should be limited to the area of cybercrime; it should not address issues relating to cybersecurity and Internet governance, which are being discussed in other forums.

However, we understand that the provisions of existing international and regional instruments should be taken into consideration in order to avoid unnecessary incompatibility with the legal systems of Member States that have used those instruments as the basis for their national legislation, or with the application of those instruments. Accordingly, it is important to draw on the experience gained in implementing the instruments in question, identifying the strengths and weaknesses that the new convention might address. The efforts of specialized groups such as the Expert Group to Conduct a Comprehensive Study on Cybercrime should likewise be taken into account.

Objectives

A new international instrument for preventing and combating cybercrime should, inter alia:

- Promote and facilitate expeditious, practical and effective international cooperation among States parties.
- Cover the prevention, detection, investigation and criminal prosecution of cybercrime offences to which the instrument applies and the collection and processing of digital evidence relating to other offences, providing States parties with the necessary tools for combating this type of transnational crime.
- Establish clearly the types of offences to which the provisions of the new convention would apply and which should be considered unlawful acts in the legal systems of all States parties.
- Promote and facilitate capacity-building in States parties that have need of such capacity-building with a view to preventing the creation of “cyberhavens”.

- Promote the sharing of good practices and lessons learned.
- Define clear rules for the establishment of jurisdiction for the purpose of requesting digital evidence from “global” Internet service providers, which is currently one of the greatest challenges to reducing impunity and supporting victims of cybercrime.
- Establish clear safeguards and a system of penalties for non-compliance with those safeguards.
- Establish sufficient powers to investigate the criminal offences covered, taking into account, at all times, respect for privacy, data protection, civil liberties and human rights.
- Given the rapid evolution of technology, the convention should have a broad and long-term vision; accordingly, technologically neutral language should be used to ensure that the applicability of the convention over time is not affected by technological developments.
- Establish a multidisciplinary approach that enables active collaboration between the public and private sectors.

Structure

- Definitions.
- Criminal offences.
- Procedural tools for investigation.
- Safeguards.
- International cooperation.
- Access to digital evidence.
- Technical assistance and building of investigative capacity.
- Standard operating procedures.
- Preventive measures.
- Implementation mechanism.

Egypt

[Original: Arabic]
[28 October 2021]

The Arab Republic of Egypt – desiring to contribute positively to international efforts to formulate a comprehensive United Nations convention on countering the use of information and communications technologies (ICT) for criminal purposes, and abiding by its commitments under national, regional and international treaties and conventions relating to human rights and the countering of transnational crime – has prepared the present submission, which includes tentative elements proposed for inclusion in the body of the aforementioned convention, in the hope of achieving the desired aims by strengthening international cooperation and formulating a common crime policy aimed at countering all ICT-related offences with a view to averting the dangers posed by these offences to the security and interests of States and the safety of their communities and citizens.

I. Objectives

The convention should aim to strengthen cooperation among the States Members of the United Nations in countering the use of ICT for criminal purposes, with a view to preventing any actions that would threaten the integrity and

confidentiality of ICT, criminalizing the misuse of ICT for illegal purposes, facilitating the means of investigating and prosecuting perpetrators. The convention should also provide for the elimination of the consequences of ICT-related offences, including the suspension of transactions relating to assets obtained as a result of the commission of any illegal act mentioned in the convention and the confiscation and return of the proceeds of such offences, by providing powers sufficient to counter ICT-related offences effectively through the establishment of international cooperation arrangements to facilitate the detection, investigation and prosecution of such offences and extradition.

II. Scope

1. Except as otherwise provided, the convention should apply to the prevention of the offences mentioned in the convention itself.

2. Each State party should take all necessary measures to establish jurisdiction over the criminal offences and other unlawful acts established as such under the convention, when the offence is:

(a) Committed in the territory of that State party; or

(b) Committed on board a ship flying the flag of that State party or on board an aircraft registered under the law of that State party at that time; or

(c) Transnational in nature, and an organized criminal group is involved in committing it. An offence should be deemed to be of a transnational nature if it was committed: (i) in more than one country; (ii) in one country, but partly prepared, planned, directed or supervised in another country; (iii) in one country by an organized criminal group engaged in criminal activities in more than one country; or (iv) in one country, but has serious consequences in another country.

3. For the purposes of implementing the convention, it should not be necessary for the offences or other illegal acts mentioned in the convention to result in material damage, except as otherwise provided therein.

4. States parties should consider restricting the declaration of reservations in order to enable broad application of the above-mentioned measures.

III. Protection of sovereignty

1. Each State party should carry out, in accordance with its national legislation and constitutional principles, its obligations arising from the application of the convention in accordance with the principles of sovereign equality of States and non-interference in the internal affairs of other States.

2. The convention should not authorize the competent authorities of a State party to exercise in the territory of another State party the jurisdiction and functions that are reserved exclusively for the authorities of that other State under its national legislation.

IV. Offences proposed to be covered by the Convention

1. Each State party should adopt such legislative and other measures as are necessary to prevent the commission of the offences mentioned in the convention or any other ICT-related offences, including blocking and removing content related to such offences; detect offences; prosecute perpetrators; extradite criminals; and facilitate procedures for international cooperation and evidence-gathering.

2. Each State party should also adopt such legislative and other measures as may be necessary to criminalize the following acts:

Article 1. The unlawful use of communication and information services and technologies, including the unlawful benefit, or abetting of the unlawful benefit of others, from telecommunications services or audio or video channels transmitted through information networks or an ICT device.

Article 2. Unlawful access and/or exceeding the limits of the right of access, including:

1. Use of a privilege granted to access a website, private account or information system in a way that exceeds the limits of the privilege in terms of time or access level.

2. Unlawful access or communication with all or part of an information technology system and the continuation of such access or communication.

3. The penalty for this offence should be increased if such access or communication results in:

(a) The erasure, modification, distorting, copying, transfer or destruction of saved data, electronic devices and systems or communication networks, or harm to users and beneficiaries;

(b) Access to confidential government information.

Article 3. The attacking of a website design by unlawfully damaging, disrupting, slowing, distorting, concealing or changing the design of the website of a company, institution, facility or natural person.

Article 4. The deliberate and unlawful interception of a data flow by any technical means or by cutting off the transmission or reception of information technology data.

Article 5. The violation of data integrity by destroying, erasing, obstructing, modifying or blocking information technology data intentionally and unlawfully.

Article 6. The misuse of information technology by producing, selling, buying, importing, distributing, providing or possessing any designed or adapted tools or software, password or similar information by which an information system may be accessed with the intent of using it to commit one of the offences mentioned in the convention, or the creation of malicious software intended for the destruction, blocking, modification, copying or dissemination of digital information, or neutralization of its security features, except for purposes of lawful research.

Article 7. Forgery using information technology to alter the veracity of information in a way that would cause harm with the intent of using the altered information as valid information.

Article 8. Fraud by causing harm to beneficiaries and users – intentionally and unlawfully – with the intention of fraud to achieve interests and benefits in an illegal way for the perpetrator or others, including through fraudulent electronic offences related to virtual currencies (digital or encrypted).

Article 9. Threat or extortion by using ICT or any other technological means to threaten or blackmail a person into committing or refraining from committing an act.

Article 10. Pornography in which:

1. ICT is used to produce, display, distribute, provide, publish, buy, sell or import pornographic materials for obscene purposes.

2. ICT is used to produce, display, distribute, provide, publish, buy, sell or import child or minor pornography materials, including possession of such materials or materials depicting children or minors indecently in ICT or on any ICT storage medium.

Article 11. Other pornography-related offences, including sexual exploitation or harassment, especially of women, children or minors.

Article 12. Encouragement of, or coercion to, commit suicide, including the encouragement or coercing of minors to commit suicide, through psychological or other pressure via information and communication networks, including the Internet, whether through direct interaction or through popular technologies or electronic games.

Article 13. The use of ICT to involve minors in the commission of illegal acts that endanger their lives or their physical or mental health.

Article 14. Use of ICT to violate privacy, including by creating an email, website or private account and falsely attributing it to a natural or legal person.

Article 15. Use of information technology to commit terrorism-related offences, including:

1. The dissemination of the ideas and principles of terrorist groups or justification of terrorism.

2. The financing of terrorist operations or training for such operations, facilitation of communication between terrorist organizations or provision of logistical support to persons who carry out terrorist operations.

3. Dissemination of methods for making explosives, especially for use in terrorist operations.

4. Spreading of fanaticism, sedition, hatred or racism.

5. States parties should take the necessary measures to prohibit the dissemination of such content on ICT means, including blocking and removing content related to these offences.

Article 16. Financial offences, such as money-laundering, and including:

1. Using ICT to commit financial offences or misuse of virtual currencies (digital or encrypted).

2. Carrying out money-laundering operations, or requesting assistance or disseminating methods for carrying out money-laundering.

Article 17. Illicit use of electronic payment instruments, including:

1. Forging, fabricating or creating by any means any device or material that facilitates the counterfeiting or imitating of any electronic payment instrument.

2. Appropriating the data of any payment instrument, using such data, providing the data to others or abetting the obtainment of such data for others.

3. Using an information network or information technology to gain unauthorized access to the code or data of a payment instrument.

4. Knowingly accepting a forged payment instrument.

Article 18. Offences related to organized crime or transnational crime committed by means of information technology, including:

1. Marketing or trafficking of narcotic drugs or psychotropic substances.

2. Illicit distribution of counterfeit medicines or medical products.

3. Smuggling of migrants.

4. Trafficking in persons.

5. Trafficking in human organs.

6. Illicit trade in arms.

7. Trafficking in cultural property.

Article 19. Offences related to infringement of copyright and related rights, including infringement of copyright and related rights as defined in the law of the State party, if the act is committed intentionally.

Article 20. Unauthorized access to critical information infrastructure, including:

1. Creating, distributing or using software or other digital information designed to provide unauthorized access to a critical information infrastructure, including the destruction, blocking, modification or copying of the information contained therein or neutralization of its security features.

2. Violating the operating rules established for media intended for the storage, processing or transfer of protected digital information contained in critical information infrastructure or information systems, or information protected under the national legislation of the State party, and communication networks that belong to critical information infrastructure, or the violation of the rules of access to them, if such violation damages the critical information infrastructure.

Article 21. Incitement to subversive or armed activity or other criminal offences, including calls issued through ICT for subversive or armed activities directed against the Government of another State that would undermine public security and stability, or calls for the commission of criminal offences punishable by imprisonment for a period of not less than one year.

Article 22. Extremism-related offences, including distributing materials that advocate or justify illegal acts based on a political, ideological, social or ethnic motives or that urge ethnic or religious hatred or enmity in general; or providing access to such materials.

Article 23. Attempted commission of any offence provided for under the convention, including participation as an accomplice in and/or organizing or directing other persons to commit any offence provided for under the convention.

Article 24. Other illegal acts.

The convention should not preclude a State party from establishing as an offence any other illegal act committed intentionally through ICT that causes substantial harm.

V. Legal liability, criminal procedures, law enforcement and international legal assistance

Article 1. Liability of legal persons

Subject to its national legislation, each State party should establish the criminal liability of a legal entity for any offences committed by its representatives in its name or for its benefit, without prejudice to the imposition of punishment on a natural person, such as the site manager, who committed the offence.

Article 2. Liability of service providers/site managers

Without prejudice to the provisions of the convention, service providers/site managers and their subordinates should abide by the following obligations, violation of which should be criminalized:

1. Saving and storing the information system log or the log of any information technology for a period to be determined. The data to be preserved and stored should include:

(a) Data that enable identification of the service user;

(b) Data related to the content of the client's information system whenever under the control of the service provider;

(c) Data related to communication traffic;

(d) Data relating to communication peripherals;

(e) Any other data specified by the State for the purposes of implementing the convention.

2. Maintenance of the confidentiality of the data that have been saved and stored and refrainment from disclosing such data without a reasoned order from a competent authority, including the personal data of any of the service users or any data or information related to the sites or private accounts accessed by such users or the persons or entities with which the users communicate.

3. Securement of data and information in a manner that maintains their confidentiality and protects them from breach and damage.

4. The service provider/site manager should provide service users and any competent authority with the following data and information in a form and manner that provides for easy, direct and continuous accessibility:

(a) The name and address of the service provider;

(b) The contact information of the service provider, including email address;

(c) Licensing data to identify the service provider and the competent authority that supervises it.

5. The service provider/site manager – if requested by the competent authorities specified by the State – should provide all technical capabilities that allow the competent authorities to exercise their powers.

Article 3. Criminal procedures

1. Each State party should take the necessary legislative and other measures to establish powers and procedures for preventing, identifying, detecting, investigating and taking legal action related to offences and other illegal acts.

2. Each State party should apply the aforementioned powers and procedures to:

(a) Criminal acts and other unlawful acts established in the convention;

(b) Other criminal offences or other unlawful acts committed by means of ICT;

(c) The electronic gathering of evidence of offences.

3. The criminal procedures should include:

(a) The expedited preservation of data stored using information technology, including traffic data that have been stored using information technology, especially if it is believed that such information is subject to loss or modification, by ordering the concerned person to preserve the integrity of the information in his/her possession or under his/her control to enable the competent authorities to search and investigate, while maintaining the confidentiality of any actions taken in this regard;

(b) The expedited preservation and partial disclosure of traffic data regardless of whether one or more service providers transmitted the information, and ensuring that the competent authorities promptly disclose a fair amount of information to enable the State party to identify the service provider and the path through which the information was transmitted;

(c) The issuance of orders to hand over information in the possession of a person in the territory of a State party and stored on an information technology or storage medium, or in the possession of a service provider that provides its services in the territory, or under the control, of the State party;

(d) The inspection of, or access to, information stored in an information technology or storage medium;

(e) The control, copying and preservation of stored information in order to complete procedures for searching and accessing the information;

(f) The real-time collection of traffic data and the obliging of the service provider within the jurisdiction to collect, record and maintain the confidentiality of the information;

(g) The interception of information content to enable the competent authorities to collect and record, through technical means, information transmitted by means of ICT in real time;

(h) Each State party should adopt the necessary legislative and other measures to enable its competent authorities to halt the transmission and broadcasting of any content that constitutes an offence under the convention.

4. Acceptance of digital evidence:

Digital evidence derived or extracted from devices, equipment, electronic media, information systems, computer programs or any means of ICT should have the value and probative force of material forensic evidence in criminal evidence when such digital evidence meets the technical conditions required under the laws of the States parties.

Article 4. International legal and judicial cooperation

1. States parties should facilitate cooperation among themselves in accordance with the convention or the principle of reciprocity to exchange information with a view to preventing the commission of information technology offences, assisting in the investigation of such offences and tracking the perpetrators thereof.

2. States parties should cooperate to the fullest extent possible in accordance with the provisions of the present article and pursuant to other international instruments on international cooperation in criminal matters and in accordance with the principle of reciprocity, as well as relevant national legislation, with a view to preventing, suppressing, detecting and prosecuting offences relating to ICT use.

3. For the purposes of extradition and mutual legal assistance in criminal matters, no offence referred to in the convention should be considered a political offence. Accordingly, a request for extradition or legal assistance in criminal matters related to such offences may not be rejected on the grounds that it relates to a political offence, an offence associated with a political offence or a politically motivated offence.

5. Jurisdiction:

Each State must adopt the necessary measures to extend its jurisdiction over the offences mentioned above, if:

(a) The offence is committed or effected in whole or in part in the territory of the State party;

(b) The offence is committed or effected in whole or in part on board a ship carrying the flag of the State party;

(c) The offence is committed or effected in whole or in part on board an aircraft registered under the laws of the State party;

(d) The offence is committed or effected in whole or in part by a national of a State party if the offence is punishable according to the national legislation at the place of its commission, or if it was committed outside the jurisdiction of any State;

(e) The offence affects one of the higher interests of the State.

6. Extradition:

(a) Offenders should be exchanged between States parties for the offences set forth above, provided the offences are punishable under the legislation of the States parties concerned. A State party whose legislation so allows may agree to a request to

extradite a person for an offence covered by the convention that is not punishable under its national legislation;

(b) The offences stipulated above should be considered extraditable offences for offenders who commit them in respect of any extradition treaty existing between the States parties;

(c) If a State party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State party with which it has no extradition treaty, the convention may be considered a legal basis for extradition;

(d) An extradition should be subject to the conditions stipulated in the legislation of the requested State party or to the conditions contained in applicable extradition treaties, including in respect of the grounds on which the State party can reject the request;

(e) Each State party may refrain from extraditing its citizens, in which case it should, within the limits of its jurisdiction, indict those of its citizens who commit, in any other State party, offences punishable under the legislation of both States parties by a penalty of deprivation of liberty, if the other State party forwards to it a request to prosecute such citizen, accompanied by the files, documents, information and evidence in its possession. The requesting State party should be informed of what has been done regarding its request, and a determination should be made of the nationality of the offender on the date of the offence for which extradition is requested;

(f) States parties should endeavour, subject to their national legislation, to expedite extradition procedures and to simplify the related evidentiary requirements in respect of any offence to which this article applies;

(g) A requested State party, subject to its national legislation and extradition treaties, may, upon being satisfied that the circumstances so warrant and are urgent, and at the request of the requesting State party, take into custody a person whose extradition is sought and who is present in its territory, or it may take other appropriate measures to ensure that such person is present at extradition proceedings;

(h) If an extradition request submitted for the purpose of executing a court ruling is refused on the grounds that the person whose extradition is sought is a national of the requested State party, the requested State party should – if permitted by, and in accordance with, its national legislation – consider, at the request of the requesting State party, the enforcement of the penalty imposed under the national legislation of the requesting party, or of any portion of such penalty still outstanding;

(i) Any person regarding whom proceedings are being conducted in connection with any of the offences to which this article applies should be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided for by the national legislation of the State party in the territory of which that person is present;

(j) Nothing in the convention should be interpreted as imposing an obligation to extradite if the requested State party has substantial grounds for believing that the extradition request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion or nationality, or that compliance with the request would cause prejudice to that person's position for any one of those reasons;

(k) States parties should not be able to refuse a request for extradition simply because the offence is an offence relating to financial matters;

(l) Before refusing extradition, the requested State party should, where appropriate, consult with the requesting State party in order to provide the latter with ample opportunities to present its views and to provide information relevant to the facts set forth in its request;

(m) Each State party should, at the time it deposits its instrument of ratification or adoption, be obliged to notify a specialized body, to be agreed upon, of the contact

information of the authority responsible for requests for extradition or procedural arrest and to update that body periodically.

7. Mutual assistance:

(a) All States parties should provide mutual assistance to the fullest extent possible for the purpose of investigations, procedures related to information and information technology offences or the gathering of electronic evidence of crimes;

(b) A request for bilateral assistance and communications related thereto should be submitted in writing. Each State party may, in emergency cases, submit an urgent request, including by email, provided such communications are reasonably secure (including the use of encryption) and referenced, and transmission is confirmed as requested by the State party;

(c) Except as provided in the convention, bilateral assistance should be subject to the conditions stipulated in the legislation of the requested party or in mutual assistance treaties, including the grounds on which the requested party may refuse to cooperate;

(d) When the State party from which mutual assistance is requested can provide assistance only if there is dual criminality, the condition of dual criminality should be considered fulfilled regardless of whether the legislation of the State party classify the relevant offence in the same category as the requesting State party.

8. Provision of information proprio motu:

A State party may, in accordance with its national legislation and without the prior request of another State party, forward information gathered during its own investigation if it believes that the disclosure of such information could help that other State party to initiate or conduct an investigation relating to offences established as such under the convention, or might result in a cooperation request from that State party.

9. Procedures related to requests for cooperation and mutual assistance:

(a) The subparagraphs of this paragraph should be applied in the absence of a mutual assistance and cooperation treaty or convention between the requesting and requested State party based on legislation in force. Should such a treaty or convention exist, then said subparagraphs should not be applied unless the concerned parties agree to apply them in whole or in part;

(b) Each State party should designate a central authority for transmitting, receiving and granting requests for mutual legal assistance or referring them to the competent authority. The contact information of the central authority should be periodically updated;

(c) Mutual assistance requests under this article should be implemented according to the procedures specified by the requesting State party, provided that they are not inconsistent with the legislation of the requested State party;

(d) The requested State party may postpone taking measures in response to the request if such measures could affect criminal investigations being conducted by its authorities;

(e) Before refusing or postponing assistance, the requested State party should determine whether to grant the request in part or subject to such conditions as it deems appropriate, after consultations with the requesting State party;

(f) The requested State party should inform the requesting State party of the results of the execution of the request. In the event that the request is refused or its final execution is postponed, the requested State party should be obliged to notify the requesting State party of the reasons for such refusal or significant postponement;

(g) The requesting State party may request the requested State party to maintain the confidentiality of a request only insofar as it is consistent with the

fulfilment of the request. If the requested State party cannot comply with the request for confidentiality, it should so notify the requesting State party. The requesting State party should then decide the extent to which the request can be fulfilled;

(h) In urgent cases, requests for mutual assistance may be sent directly to the judicial authorities in the requested State party from their counterpart in the requesting State party. In such cases, a copy of the request must be sent at the same time by the central authority in the requesting State party to its counterpart in the requested State party;

(i) Communications and requests undertaken under the preceding subparagraph may be made through the International Criminal Police Organization (INTERPOL);

10. Refusal to provide assistance:

(a) A requested State party may refuse to provide assistance if it believes that the execution of a request would violate its sovereignty, security, order or basic interests, in addition to refusing to provide assistance on the grounds for refusal mentioned in the above paragraphs;

(b) A request for legal assistance in the offences mentioned in the convention should not be refused on the basis that the offences are political offences or the like.

11. Confidentiality and limitations of use:

In the absence of a treaty or convention on mutual assistance between the requesting and requested States parties based on legislation in force, this article must be applied. It should not be applied if such convention or treaty exists, unless the concerned States parties agree to apply it, all or in part.

12. Expedited preservation of information stored on information systems:

(a) Any State party may request another State party to urgently preserve information stored using information technology located within its territory regarding which the requesting State party would like to submit a request for mutual assistance in order to search, seize, secure or disclose the information;

(b) A requested State party may refuse to implement a preservation request if it believes doing so would threaten its sovereignty, security, order or interests.

13. When the requested State party discovers – in the context of executing a request to preserve traffic data regarding certain communications – that a service provider from another State was involved in the transmission of the information, it should disclose to the requesting State party a sufficient amount of traffic data to make it possible to identify that service provider and the path through which the information whose preservation is sought was transmitted.

14. Bilateral cooperation and assistance related to access to stored information technology information:

(a) Any State party may request another State party to search, access, seize, secure or disclose information technology information stored and located within the territory of the requested State party, including information that has been preserved;

(b) The requested State party should be obliged to comply with the requesting State party in accordance with the provisions of the convention;

(c) The response to the request should be on an urgent basis if the relevant information is subject to loss or modification.

15. Cross-border access to information technology information:

Any State party may, without obtaining the authorization of another State party, access information technology information that is publicly available (open source), regardless of the geographical location of the information.

16. Bilateral cooperation and assistance regarding the real-time collection of traffic data:

(a) States parties should provide bilateral assistance to each other regarding the real-time collection of traffic data associated with certain communications in their territories and transmitted by means of information technology;

(b) Each State party should provide such assistance, at least for offences in which the real-time collection of traffic data is available for similar cases under national legislation.

17. Bilateral cooperation and assistance regarding data on content:

States parties should be obliged to provide bilateral assistance to each other in connection with the real-time collection of content data for specific communications transmitted by information technology to the extent permitted by applicable treaties and national legislation.

18. Specialized agency:

(a) Each State party should ensure, in accordance with the basic principles of its legal system, the existence of a specialized agency, dedicated around the clock, seven days a week, to ensuring the provision of immediate assistance for the purposes of investigations or procedures related to information technology offences or to collect evidence in electronic form in a particular offence. Such assistance should include facilitating or implementing:

(i) The provision of technical advice;

(ii) The preservation of information based on relevant articles;

(iii) The gathering of evidence, provision of legal information and determination of the location of suspects;

(b) The specialized agency in any State party should have the ability to communicate with similar agencies in other States parties on an urgent basis;

(c) If the specialized agency designated by any State party is not part of the authorities of that State party that are responsible for international bilateral assistance, the specialized agency should be empowered to coordinate with those authorities expeditiously;

(d) Each State party should ensure the availability of qualified human resources to facilitate the work of the aforementioned agency.

VI. Technical assistance and training

1. General principles of technical assistance:

(a) States parties should consider affording one another the widest measure of technical assistance, especially for the benefit of developing countries, for their respective plans and programmes to combat ICT-related crimes, including material support and training in the areas referred to in the convention, as well as training, assistance, transfer of technology and knowledge and the exchange of best relevant experiences and expertise, which will facilitate international cooperation between States parties on extradition and mutual legal assistance;

(b) States parties should strengthen efforts to maximize the effectiveness of operational and training activities in international and regional organizations and in the framework of relevant bilateral and multilateral agreements or arrangements;

(c) States parties should consider assisting one another, upon request, in conducting evaluations, studies and research relating to the types, causes and effects of ICT-related crimes committed in their respective countries, with a view to developing, with the participation of the competent authorities and main actors, strategies and action plans to combat these types of offence;

(d) States parties should consider establishing financing mechanisms with a view to providing assistance through technical assistance programmes and projects to efforts made by developing countries;

(e) States parties should consider exchanging information on legal, policy or technological developments related to cybercrime and the gathering of evidence in electronic form.

2. Training and capacity-building:

(a) Each State party should, as necessary, develop, implement or improve specific training programmes for the staff responsible for preventing and combating ICT-related crimes. Such training programmes could cover the following areas:

(i) Effective measures to prevent, detect and investigate ICT-related crimes, as well as to punish and combat them, including the use of electronic evidence-gathering and investigative techniques;

(ii) Prevention of the transfer of proceeds of offences established as such under the convention, and recovery of such proceeds;

(iii) Detection and blocking of transactions related to the transfer of proceeds of offences established as such under the convention; surveillance of the movement of proceeds of offences established as such under the convention; and surveillance of the methods used to transfer, conceal or disguise such proceeds;

(iv) Establishment of appropriate and efficient legal and administrative mechanisms and methods to facilitate the seizure and confiscation of proceeds of offences established as such under the convention;

(v) Methods used in protecting victims and witnesses who cooperate with judicial and law enforcement authorities;

(vi) Development and planning of a strategic policy to counter ICT offences. Countries should invest in building and strengthening digital forensics capabilities, including providing security training and qualification, as well as information security management systems to support successful cybercrime prosecutions through the examination of electronic devices in order to collect evidence in a reliable manner;

(vii) Preparation of requests for mutual legal assistance that meet the conditions provided for in the convention;

(viii) The investigation of cybercrimes, electronic evidence handling, chain of custody and forensic analysis;

(ix) Provision of language and professional training in all activities related to countering ICT-related offences and protecting and expediting communication with specialized agencies to detect and control related offences;

(b) States parties that have more advanced capabilities and infrastructure in the field of cybercrime should assume responsibilities commensurate with those capabilities when providing legal assistance to other States, especially developing countries, and in providing support and advice and transferring knowledge to them in the area of countering cybercrime.

European Union and its member States

[Original: English]
[2 November 2021]

This document reflects the views and position of the European Union and its member States[1] on the scope, objectives and structure (elements) to be taken into account in elaborating a new United Nations convention on countering the use of information and communications technologies for criminal purposes and to contribute to the preparation of the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established for that purpose in accordance with General Assembly resolution 74/247.

This contribution is without prejudice to any future positions that the European Union and its member States may take during the course of future negotiations on the scope, objectives and structure of a future United Nations convention.

I. Objectives

The European Union and its member States underline that a future United Nations convention should serve as a practical instrument for criminal law enforcement and judicial authorities in the global fight against cybercrime, with the aim of adding value to international cooperation. As reflected in General Assembly resolutions 74/247 and 75/282, a future United Nations convention should take into full consideration the existing framework of tried-and-tested international and regional instruments in the field of organized crime and cybercrime. Therefore, any new convention should complement and avoid impairing in any way the application of existing instruments or the further accession of any country to them, and, to the extent possible, avoid duplication.

A future United Nations convention should provide for the protection of human rights and fundamental freedoms, which apply both offline as well as online, and be compatible with relevant instruments in that area.

A future United Nations convention, as agreed by the General Assembly in its resolution 75/282, should take into full consideration the work[2] and outcomes[3] of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.

II. Scope

To that end, the European Union and its member States believe that the scope of a future United Nations convention should be focused primarily on substantive criminal law and criminal procedural law, as well as associated mechanisms for cooperation. It should also comply with international human rights standards and strive to fight cybercrime in the most effective manner and thus protect victims.

The European Union and its member States consider that this new instrument should precisely define the terms it uses and give preference to concepts already agreed in existing international texts.

The European Union and its member States recommend that the content of this convention be compact and focus on the essential elements of criminal justice, and should thus exclude as much as possible any ancillary elements.

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

[2] See www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html.

[3] See UNODC/CCPCJ/EG.4/2021/2.

On the basis of the principles outlined above, the European Union and its member States consider that the following elements should be included in a future United Nations convention:

1. Substantive criminal law provisions linked to cybercrime offences that should be criminalized by all States parties to a future United Nations convention. These provisions should in general relate only to high-tech crimes and cyber-dependent crimes, such as illegally gaining access to, intercepting or interfering with computer data and systems.[4]

Substantive criminal law provisions must be clearly and narrowly defined and be fully compatible with international human rights standards and a global, open, free, stable and secure cyberspace. Vague provisions criminalizing types of behaviour that are not clearly defined in a future United Nations convention or in other universal legal instruments would risk unduly and disproportionately interfering with human rights and fundamental freedoms, including the right to freedom of speech and expression, while also resulting in legal uncertainty.

Provisions of substantive criminal law should, to the extent possible, be drafted in a technologically neutral manner in order to encompass technical developments in the future.[5] At the same time, the exchange of views and information about new challenges posed by further technological developments should be encouraged.

Incompatibility with other international conventions must be avoided, in particular where certain offences, such as arms trafficking or the illicit distribution of narcotic drugs, are already widely covered by existing provisions in international conventions, such that the inclusion of these types of behaviour in a convention on cybercrime would not be of added value.

In general, a future United Nations convention should refrain from setting (minimum) standards for sanctions or punishment for specific offences beyond existing models, such as article 11, paragraph 1, of the United Nations Convention against Transnational Organized Crime.

As regards rules on jurisdiction, a future United Nations convention should be modelled on the approach set out in existing legal instruments, such as in article 15 of the Organized Crime Convention.

2. Appropriate substantive and procedural conditions and safeguards to ensure compatibility with human rights and fundamental freedoms, including the principles of legality, necessity and proportionality of law enforcement action and specific substantive and procedural guarantees ensuring, in particular, the right to privacy and personal data protection, the right to freedom of expression and information and the right to a fair trial. Such guarantees should build on and be on at least the same level as the safeguards included in other relevant international legal instruments.

3. Procedural measures and criminal procedural provisions regarding mechanisms for cooperation between the parties to a future United Nations convention, including cooperation in investigations and other judicial proceedings and in obtaining electronic evidence, where appropriate and relevant, while ensuring it can be collected, preserved, authenticated and used in criminal proceedings.[6] Such measures and provisions would need to be consistent with and build on the models provided by those included in other relevant international legal instruments and be complemented by appropriate guarantees, including of cooperation in emergency situations.

[4] In line with recommendation 5, on criminalization, adopted by the Expert Group to Conduct a Comprehensive Study on Cybercrime at its meeting held in Vienna from 6 to 8 April 2021 (see UNODC/CCPCJ/EG.4/2021/2, annex, recommendation 5).

[5] See UNODC/CCPCJ/EG.4/2021/2, annex, recommendation 1, on legislation and frameworks.

[6] Ibid., recommendation 16, on electronic evidence and criminal justice.

4. Elements, in conformity with human rights, regarding **capacity-building, the sharing of best practices and lessons learned, and technical assistance**, including the significant role of the United Nations Office on Drugs and Crime in these areas**.**

The European Union and its member States consider that the following must be excluded from the scope of a future United Nations convention:

- Matters related to or regulating national security or State behaviour
- Matters related to or regulating rules on Internet governance, which are already being addressed in the context of dedicated multi-stakeholder policies and forums

Finally, as an intergovernmental instrument, a future United Nations convention should refrain from directly imposing obligations on non-governmental organizations, including those in the private sector, such as Internet service providers.

III. Structure

On the basis of the above, a future United Nations convention could include the following different chapters:

Preamble (scope and objectives of a future United Nations convention)

I. Types and precise definitions of crimes

II. Domestic procedural rules, and fundamental principles to be respected in that regard, for example, respect for human rights, including the rights to privacy and personal data protection, necessity and proportionality

III. International cooperation

IV. Technical assistance, training and capacity-building, and role of the United Nations Office on Drugs and Crime in that regard

Indonesia

[Original: English]
[28 October 2021]

General background and objectives

As one of the world's largest Internet users, Indonesia recognizes the importance of information and communications technology (ICT) for society. However, advances in ICT have been exploited for irresponsible behaviour, most notably cybercrime and cyberterrorism, undermining the use of ICT for political, economic and social development.

Cybercrime, like other transnational crimes, has affected the international community, owing to the unique and borderless nature of technology and cyberspace. Thus, international cooperation is critical. Indonesia commends the adoption of General Assembly resolution 74/247, in which the Assembly decided to establish an open-ended ad-hoc intergovernmental committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

Indonesia believes it is very timely and critical to discuss the specific cybercrime convention within the framework of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, and hopes that States will build on the momentum to discuss and negotiate an international instrument capable of responding to cybercrime challenges, in an inclusive and transparent manner.

Over the last decade, significant progress has been made in the discussion and development of international instruments aimed at determining the most effective methods of cybercrime prevention. As a result, when considering a future cybercrime instrument, States should consider all existing platforms and frameworks, including the work of the intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime and the United Nations Convention against Transnational Organized Crime.

The discussion on the cybercrime convention should primarily aim at enhancing and promoting international cooperation in support of national, regional and international efforts to combat the use of ICTs for criminal purposes, including by providing technical assistance to improve the national legislation and frameworks of Member States and build the capacity of national authorities to deal with such crimes.

Furthermore, the convention should provide for appropriate and effective measures between and among States, as well as, as applicable, in collaboration with relevant international and regional organizations.

Principles

As with many international conventions, our consideration should reflect Member States' obligations in accordance with the principles of sovereign equality and territorial integrity of States, as well as non-interference in the domestic affairs of other States. Furthermore, States should respect the sovereign rights of other States when developing policies and legislation to fight cybercrime in accordance with their national conditions and needs.

The future instrument must recognize the impact on security and the socioeconomic and humanitarian consequences of the use of ICTs for criminal purposes. At the same time, the convention must ensure that measures to combat cybercrime focus on the criminal behaviour and do not jeopardize the development of ICTs, including research, development and technology transfer.

It is in the interest of all and vital to the common good to promote the use of ICTs for peaceful purposes. Respect for sovereignty, human rights and fundamental freedoms, as well as sustainable and digital development, remain central to these efforts.

Indonesia also sees the merit of ensuring that criminal procedures are established, implemented and applied in accordance with each nation's domestic law, while also acknowledging the need to address challenges posed by the differences in the criminal procedures of States, as well as each State's obligations under relevant international instruments, such as the Organized Crime Convention and treaties on international human rights, intellectual property rights, and bilateral extradition and mutual legal assistance.

Furthermore, Member States must stress the need to maintain an open and transparent multi-stakeholder process that allows all Member States to negotiate in good faith towards informed, consensus-based and realistic solutions.

Scope

The scope of the convention must be able to address current and future challenges posed by the misuse of ICTs for criminal purposes, protect ICT users, and mitigate and prevent harm to people, data, systems, services and infrastructure.

The convention should also be able to ensure that Member States are able to adopt legislative and other measures as may be necessary to establish as criminal offences the undertaking of activities prohibited by the convention, in particular computer crimes and computer-related crimes, and for further illegal ends.

Indonesia believes that the future convention should cover a whole range of core cybercrime offences. These include but are not limited to:

(a) Illegally accessing or hacking into computer systems;

(b) Illegal interception of computer and system data;

(c) Fraud;

(d) Misuse of computer data and systems for criminal purposes;

(e) Infringement of copyright and related rights;

(f) Manipulation of computer data and systems;

(g) Distribution and transmission of illegal content and materials, for example, pornography, child pornography, disinformation, conspiracies, hoaxes and material that contains racially-, nationality-, religion- or politically-based hostility.

Member States should consider adopting the measures required to carry out the criminal proceedings outlined in the convention, including but not limited to:

(a) Data and system preservation and the preservation of traffic data stored by single or multiple service providers, and noting that the time frame for the preservation of data and the classification of stored data in their territory are regulated under national and domestic law;

(b) The submission or transfer of stored computer data by individuals or legal entities, and establishing adequate measures to compel online system service providers to submit or transfer stored computer data, including data related to the type of services provided;

(c) Search and seizure of data and computer systems, the creation and preservation of copies of computer data, and the modification and transfer of stored data;

(d) The collection and recording of real-time traffic data, as well as obtaining traffic data from online service and/or system providers.

Taking this into account, Member States should ensure that the cybercrime investigation process is carried out in accordance with the principles of privacy protection, confidentiality, public service sustainability, maintaining the continuity of public services and upholding the public interest, as well as data integration.

Cooperation

Cybercrime and crimes facilitated by the use of ICTs should be investigated effectively at the national level and transnationally. Thus, the instrument should serve as an effective mechanism for international cooperation in combating the use of ICTs for criminal purposes. Such collaboration should be implemented on the basis of mutual benefit and reciprocity in accordance with national legislation, taking into account existing instruments and ongoing mechanisms and frameworks.

Given the importance of multi-stakeholder approaches to the prevention, detection and eradication of cybercrime, the discussion should also focus on fostering strong cooperation with entities dealing with cybercrime, including cooperation between law enforcement authorities and ICT service providers. In this context, collaboration with private enterprise, reinforced by public-private partnerships when feasible, is crucial for improving knowledge and increasing the effectiveness of cybercrime responses. Member States should also invest in raising awareness of cybercrime in the public and private sectors.

Our deliberations should also highlight measures to allow authorities to conduct investigations in which data are gathered and confiscated through mutual legal assistance mechanisms, and Member States may wish to consider using their existing legal frameworks in this regard.

In regard to mutual legal assistance, our deliberations should take into account to the fullest extent possible relevant laws, treaties and agreements, with respect to investigations, prosecutions and judicial proceedings. Member States are encouraged

to, inter alia, discuss arrangements to expedite the collection of electronic evidence or information-sharing mechanisms between relevant authorities.

The provisions on international cooperation in this convention must provide an essential legal framework for addressing procedural challenges, gaps and insufficient mechanisms in international cooperation, especially in relation to investigations, information-sharing, the collection of data and electronic evidence, and prosecution, as well as for facilitating extradition among States. Member States are also encouraged to appoint contact points or authorities to expedite the implementation of the provisions on international cooperation of the convention.

Furthermore, Member States may wish to consider strengthening their national capacity to detect, investigate and respond to the use of ICTs for criminal purposes, through capacity-building and technical assistance efforts that contribute to increasing the resilience of Member States. These capacity-building measures should be based on mutual trust, be driven by demand that corresponds to nationally identified needs and be in full recognition of national ownership.

As collaboration in preventing and eradicating cybercrime remains a priority in our discussions, the future instrument should, at the very least, include a list of activities to improve cooperation through the following measures:

(a) The sharing of information on cybercrime threats;

(b) The fostering of enhanced cooperation and coordination among law enforcement agencies, prosecutors and judicial authorities;

(c) The sharing of best practices and experiences related to the cross-border investigation of cybercrime;

(d) Engagement with service providers through public-private partnerships in order to establish modalities of cooperation in law enforcement, cybercrime investigations and evidence collection;

(e) The development of guidelines for service providers to assist law enforcement agencies in cybercrime investigations, including with regard to the format and duration of preservation of digital evidence and information;

(f) The development of human skills and human resources in policies enabling Member States to increase adaptability to digital technologies;

(g) The strengthening of the technical and legal capacities of law enforcement agencies, judges and prosecutors through capacity-building and skill development programmes.

Through this mechanism, Member States should also continue to improve the effectiveness of domestic inter-agency coordination and synergies, including information-sharing and engagement with regional organizations, the private sector, computer emergency response teams and computer security incident response teams, civil society organizations and other stakeholders to facilitate efficient international cooperation.

The discussion should also include a mechanism for reviewing the application or implementation of all commitments and obligations under the future instrument.

Jamaica

[Original: English]
[29 October 2021]

Pursuant to the request of the secretariat of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes for States to provide comments on the scope, objectives and structure of an international convention on countering

the use of information and communications technologies for criminal purposes, the following views are being submitted.

Jamaica looks forward to cooperating with other Member States to contribute to the work being undertaken to draft a convention on cybercrime. Jamaica is expecting a convention that will serve the global community by seeking to protect citizens from cyberthreats or other criminal attacks and that will receive universal acceptance and ratification. Jamaica welcomes the involvement of civil society experts in the field to inform our deliberations.

Jamaica views this process of developing a convention on countering the criminal use of information and communications technologies (ICTs), as an important step in the global response to the problems States experience because of this threat. The objective of such a convention was aptly outlined in the 2015 consensus report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, which provided, in paragraph 13, subparagraph (d), that States should consider how best to cooperate to exchange information, assist each other, prosecute the criminal use of ICTs and implement other cooperative measures to address such threats.[7]

Cooperating to exchange information to assist States in combating and prosecuting the criminal use of ICTs ought to be the overarching objective of the convention. Flowing from this is the objective of increasing understanding among States about the varying perspectives on cybercrime. It is hoped that this will lead to the harmonization of approaches, creating an international framework that will work for all. The success of this objective, however, depends on a process that considers the positions of all States, including small island developing States, in a balanced, fair, transparent and inclusive manner.

Account should be taken of other processes that can contribute to, but will not unduly delay, making progress towards concluding a convention. The timelines agreed for negotiations and completion of the draft convention should be adhered to as a demonstration of how seriously we take the combating of cybercrime.

It is understood that the definition of terms is the starting point of the negotiations. Terms establish the scope of the convention and are important for achieving the shared objectives of the participants. As such, definitions should be clear, distinct and carefully crafted to ensure that they are not unduly restrictive or broad but are suitable for the context and purposes of the convention.

Countering the use of ICTs for criminal purposes is a broad mandate. The offences must therefore be “future-proof”. They ought to be framed in a manner that does not limit the meanings to existing technologies, but instead ought to be capable of being interpreted sufficiently to keep pace with future technologies and the constantly evolving ICT environment.

The convention should feature offences that strengthen the toolkits available to countries to target cybercrime and that do not infringe upon the fundamental rights and freedoms of persons but seek to promote the observance of and respect for these rights. Consideration should therefore be given to international treaties on human rights.

The provisions of a new convention should have due regard to the principle of State sovereignty, as well as other principles outlined in the United Nations Charter and international law, on matters of criminal procedure, enforcement and international cooperation.

Jamaica believes that international cooperation must be adequately addressed in the convention, as this would encourage increased collaboration in the global fight against cybercrime. Where no mutual legal assistance treaty exists between States,

[7] A/70/174.

the convention ought to guide States on the process of making and responding to requests. This should include matters such as the responsibility for costs.

The convention must recognize the diverse capacities of States, which in turn have an impact on their ability to cooperate as extensively as would be required for optimal results. It is therefore crucial that technical assistance be made available to build the capacity of States to contribute more to the global framework against cybercrime. In this regard, capacity-building should be sustainable, have a clear purpose, correspond to domestic needs and meet the objective of human resource development in this specialized area. Consideration should also be given to establishing a funding mechanism to support capacity-building for the implementation of the cybercrime convention.

Japan

[Original: English]
[29 October 2021]

Japan, as a Member State that attaches importance to realizing an inclusive, transparent and fair process for the drafting of the forthcoming United Nations convention on cybercrime, is pleased to provide input for the new convention before the formal drafting begins and appreciates the Chair's initiative in providing this opportunity.

Although different States face different cybercrime challenges, Japan recognizes that cybercrime is a constantly evolving and common serious threat for all Member States. In order to combat cybercrime, which easily transcends national borders, it is vital to ensure that all Member States cooperate with one another. Therefore, Japan believes that we should aim to ensure a free, fair and secure cyberspace and enhance our capability to prevent and combat cybercrime all over the world by making the substance of the new international convention universal and agreeable to all Member States.

These inputs outline the views of Japan on the scope, objectives and structure of the new convention, so as to promote discussion within the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established in accordance with General Assembly resolution 74/247.

Scope

In order to strengthen global measures to combat cybercrime and to establish a universal international framework, the international community should, in the first place, develop a solid framework, focusing on basic and essential provisions on criminal offences and criminal procedure, as well as mutual legal assistance and other international cooperation in this field.

The acts that the new convention criminalizes should be limited to cybercrime; the offences established in the new convention should foremost cover cyber-dependent crimes, and cyber-enabled crimes should be covered only where it is necessary and there is broad consensus among Member States.

The new convention should be firmly based on previous and current discussions under the existing frameworks for combating cybercrime, while taking into account the discussions and work in other forums involving discussions on cybercrime, with the aim of avoiding duplication or the undermining of the work.

In order to establish a universal international framework that is generally applicable to every kind of usage of information and communications technologies, irrespective of differences between States, and to respond to the future development of technologies, the provisions in the new convention should be formulated in a way that is technologically neutral.

Despite the significance of combating cybercrime, measures against cybercrime must not be detrimental to the principle of due process or impose unjustifiable restrictions on human rights. Such safeguards are preconditions for successful international cooperation, and therefore the new convention should include concrete provisions for ensuring due process and human rights.

Objective

The primary objective of the new convention should be to contribute to the safety and security of everyone involved in information and communications technologies that should be protected, and to the protection of their interests. This can be achieved by globally enhancing measures against cybercrime through establishing a universal international framework with the broadest application to cybercrime in its various transnational forms and supporting effective bilateral or multilateral cooperation in criminal investigations and prosecutions.

In order to achieve this objective, the new convention should stipulate basic and essential provisions that can be complied with and implemented by as many Member States as possible, thereby raising the worldwide level of measures against cybercrime and strengthening the existing frameworks.

Structure

Japan believes that the following basic structure would be effective in organizing the new convention, but supports being flexible with regard to a more detailed structure in the upcoming negotiations:

(a) Definition of terms;

(b) List of domestic measures that Member States should adopt:

(i) Criminalization:

a. Offences categorized as cyber-dependent crimes;

b. Offences that should be criminalized among cyber-enabled crimes;

(ii) Procedural provisions regarding the preservation, disclosure and production of data;

(iii) Safeguards for securing human rights and other interests;

(c) International cooperation in extradition, mutual assistance and other forms of cooperation;

(d) Final provisions.

Jordan

[Original: Arabic]
[28 October 2021]

Scope

The convention should cover offences related to:

- Confidentiality, integrity and availability of electronic services.
- Unauthorized access to an information network, information system or any part thereof.
- Disruption of critical infrastructure.
- Intent to sabotage information networks or information systems.
- Spying on the flow of data on an information network or information system.
- Fraud, forgery and impersonation.

- Interception of financial systems data or information.
- Violation of privacy and intellectual property.
- Hardware, decryption software and access codes.
- Internet address fraud.
- Pornography.
- Exploitation and abuse of children.
- Dissemination of false news.
- Racial discrimination.
- Exploitation and abuse of women.
- Sedition, incitement or spreading of hate speech.
- Illegal trafficking through information networks or websites.
- Dissemination, support or promotion of a terrorist ideology.
- Use of ICT for terrorist purposes.
- Insulting of religions, countries and symbols.
- Supply chains.
- Ransomware.
- Electronic phishing.
- Software piracy.
- Unauthorized use of data by service providers.

Objectives

The objectives of the convention should be to:

- Strengthen international cooperation and coordination to counter the use of ICT for criminal purposes.
- Develop international legislation to counter the use of ICT for criminal purposes.
- Highlight the importance of protecting critical infrastructure by countering the use of ICT for criminal purposes.
- Promote the importance of building and improving national and international capacities and raise the level of awareness of individuals and societies about countering the use of ICT for criminal purposes.

Structure

- Introduction.
- Definitions.
- Objectives.
- Scope.
- Duties and responsibilities.
- International cooperation.
- Capacity-building and awareness-raising.
- Implementation mechanism.
- Continuous updating of the convention according to developments.

The convention should be broad in scope, covering the largest possible number of countries in the world, with a focus on countries that are major technology incubators.

It should include agreed international concepts concerning information technology offences against persons or funds.

The focus should be on creating ways for the law enforcement authorities of the States parties to share information with each other and establishing mechanisms for tracking funds resulting from electronic fraud offences and for identifying the digital identity of the perpetrators of such offences, in accordance with national legislation and with respect for privacy.

Permanent points of contact should be established among the States parties to respond immediately in cases of terrorism or the sexual exploitation of children, among others. It is also necessary to create mechanisms to promote cooperation with international social media companies to provide the technical information needed to counter this type of offence.

International cooperation should be promoted for building capacity among the staff of cybercrime units in the States parties through training courses, workshops and the exchange of experiences.

Kuwait

[Original: Arabic]
[17 September 2021]

1. The overall main presentation of the draft convention should stress that the convention is intended to enhance and strengthen cooperation to counter and reduce the risks of information technology offences based on the sovereign equality of States and non-interference in their internal affairs, including procedures related to the exercise of jurisdiction, respect for the rule of law, preservation of public order and security, and respect for social values.

2. The scope of the convention should take into account international instruments to prevent terrorist acts and the United Nations Convention against Transnational Organized Crime and the protocols thereto, to include offences committed in more than one country, offences prepared, planned, directed or supervised in other countries, offences committed in other countries, or offences committed in one country but having serious consequences in another country.

3. The acts to be criminalized under the convention should be established in line with the newly emerging forms of ICT-related crime defined as predicate offenses in the national legislation of the States parties, with special attention to offences related to content, hate speech and violence.

4. Frameworks should be established for the following: legal and judicial cooperation, extradition of criminals, the exchange of information, the permissibility of providing information without prior request if the State party believes that disclosure of such information could help in initiating investigations into offences, cooperation on the urgent disclosure and preservation of information stored using information technology, access to cross-border information technology, bilateral cooperation and assistance regarding the real-time collection of traffic data, the establishment of confidentiality elements, and limits on the use of data that are the subject of mutual assistance.

5. Frameworks should also be established for assessing implementation of the convention according to mechanisms applied by the States parties. Relevant institutions and points of contact of the States parties should be designated, and efforts should be made to benefit from existing information networks within the United Nations Office on Drugs and Crime.

Liechtenstein

[Original: English]
[28 October 2021]

Liechtenstein wishes to thank the secretariat of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and the Chair, H.E. Ms. Faouzia Boumaiza, for seeking the opinion of Member States on the scope, objectives and structure (elements) of the new convention. The general position of Liechtenstein is as follows.

A major objective of Liechtenstein is to ensure that a new cybercrime convention is in accordance with existing international and regional instruments, including the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime, and underpinned by international law, including human rights law.

Liechtenstein is therefore aiming for a short, functional convention that focuses on crimes that are specific to cyberspace, such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud and offences related to infringement of copyright and child pornography. Far-reaching criminalization of other types of crime outside the area of specific crimes in cyberspace should be covered in other conventions and forums and is therefore to be rejected. Furthermore, Liechtenstein opposes a duplication of offences that are covered by other specific treaties.

Owing to the rapidly changing environment in cyberspace, Liechtenstein strives for a convention that uses technically neutral language so that substantive criminal offences may be applied to both current and future technologies involved. Extensive technical definitions of specific types of cybercrime are likely to become obsolete in the future and should therefore be avoided in the convention.

Another central aspect for Liechtenstein is data protection provisions and human rights, which must have a strong place in the convention. It is paramount that data protection and human rights standards are fully respected.

A more detailed position of Liechtenstein will be presented during the negotiations for the new cybercrime convention.

Mexico

[Original: Spanish]
[21 October 2021]

For the Government of Mexico, information and telecommunications technologies, digital platforms and the cyberenvironment offer great opportunities to strengthen development, close inequality gaps and promote inclusion, well-being, justice and rights.

However, Mexico recognizes that the commission of offences and the growth of an illicit market through these technologies represent a growing concern for Governments, businesses, civil society organizations and all individuals.

International cooperation and mechanisms for legal assistance and information exchange are needed more than ever before. Mexico is committed to multilateralism and especially to the role of the United Nations in generating comprehensive and meaningful responses to this global challenge.

Mexico considers that the mandate given by the General Assembly for the elaboration of a comprehensive convention on countering the use of information technologies for criminal purposes represents an ideal opportunity to achieve a substantive, committed, plural, inclusive and transparent process that draws on the

lessons learned from other United Nations processes related to the topic and from other relevant regional experiences.

The Government of Mexico hopes that the following points will guide the process of elaborating and determining the content of the future convention.

Approach, scope and type of convention

The convention should be a comprehensive, binding legal instrument, covering both substantive and procedural matters and aimed at establishing a framework for international cooperation and the sharing of information, experience, expertise and best practices.

It is hoped that the convention will help to promote standards in order to improve investigation, mitigation and prosecution, and that, while the convention does not preclude the conclusion of other international instruments dealing with the same subject, it will serve as a benchmark for a harmonized framework that will make the prosecution of cybercrime offences more effective.

It should incorporate the following:

- General definitions, basic typologies and competent actors.
- The basic procedural measures that States should have in place for the proper investigation and prosecution of cybercrime offences.
- General criminal offences that should be considered by national legislators.
- Mechanisms for access to information and for promoting effective collaboration.

The future convention should also provide for the formulation of reservations and interpretative declarations and for a flexible amendment procedure to facilitate its updating, and establish mechanisms for settling disputes. It would be desirable to make entry into force conditional upon the deposit of 50 instruments of ratification.

Once the content of the convention is defined, it would be advisable to agree on an effective, universal implementation review mechanism that is based on peer review and does not impose a burden on States.

Relevance of other international instruments

For the Government of Mexico, it is important that the convention be based on the affirmation that international law is applicable to cyberspace and that, accordingly, existing international legal instruments such as the following be taken into consideration:

- The United Nations Convention against Transnational Organized Crime and the three protocols thereto.
- The Statute of the International Court of Justice.
- The Council of Europe Convention on Cybercrime.
- Treaties on the protection and cross-border flow of personal data.
- International treaties on human rights and treaties that safeguard the guarantees of persons involved in judicial proceedings.
- Treaties applicable to intellectual property.
- Bilateral treaties on extradition, mutual legal assistance in criminal matters and other forms of international legal cooperation.

Furthermore, the negotiation process could usefully be guided by documents adopted within the United Nations and other relevant international forums, chiefly the following:

- Compilation of conclusions and recommendations emanating from the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020.
- Final report of the 2019–2021 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace and the previous reports of 2013 and 2015.
- Final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.
- Draft guidelines for utilization of the Global Cybersecurity Agenda developed by the International Telecommunication Union.
- General Assembly resolutions on the right to privacy in the digital age.
- Human Rights Council resolutions relating to the promotion, protection and enjoyment of human rights on the Internet.

Cybercrime offences/criminal conduct that should be addressed

The Government of Mexico is of the view that the convention should highlight acts that are recognized in international law as illicit (in the terms provided for in other treaties adopted within the framework of the United Nations) and are carried out by electronic means.

While it is not expected that the convention will include an exhaustive catalogue of offences, nor that all the typologies will be compatible with the different legal systems, it is desirable that the drafting process generate dialogue as a general point of reference for the following:

- Identify theft and phishing.
- Fraud and extortion.
- Use of ransomware.
- Malware and criminal conduct related to the production, storage, distribution, sale and execution of malicious code.
- Exposure of personal or institutional information, to the detriment of its owners.
- Offences related to trafficking in persons, child pornography and violations of sexual privacy.
- Grooming and cyberbullying.
- Digital violence, including gender-based violence and violence based on hate, race, nationality, religion or political hostility.
- Methods of attack (phishing, vishing, smishing, pharming).
- Offences against national sovereignty, such as terrorism, sabotage, espionage and intrusion into systems containing information that is classified for national security reasons.
- Criminal acts targeting critical information infrastructure and the confidentiality, integrity and availability of information.
- Offences against children and adolescents.
- Violation of freedom of expression.
- Offences against intellectual property.
- Offences against the financial system.
- Illegal sale of weapons, animals, controlled medicines and medicines that are not registered health products.
- Currency counterfeiting and forgery of official documents.

- Use of cryptocurrencies and of dual-use assets for criminal purposes.
- Illegal modification of portals (defacement).
- Liability of legal persons.

It would also be appropriate to discuss, when drafting the convention, the possibility of providing for penalties for attempt and of establishing aggravating circumstances entailing harsher penalties.

Aspects relating to sovereignty and jurisdiction

- Reaffirm respect for national sovereignty and the principle of non-interference in the internal affairs of other States.
- Establish general rules for determining jurisdiction, drawing on similar provisions in other legal instruments and processes.
- Formulate common measures for obtaining traffic and content data while preventing the unlawful blocking or interception of data.
- Develop mechanisms that create certainty with regard to obtaining, retaining, preserving and submitting digital evidence.
- Clarify investigative steps such as subpoenas or arrests.
- Develop provisions governing the submission of technical and content data in criminal investigations and the prompt disclosure of computer data.
- Address the legal obligation of technology operators, service providers and Internet content providers, regardless of their physical location, to provide information to the competent authorities during investigations.

Aspects relating to information-sharing and international cooperation

The Government of Mexico considers that one of the main objectives of the convention should be to create certainty with regard to information-sharing and international cooperation and to establish processes for its effective implementation. It is hoped that, among other aspects, the following will be addressed:

- Mutual legal assistance.
- Extradition.
- Common mechanisms for requesting, responding to, receiving and exchanging information for investigative and intelligence purposes.
- Judicial oversight procedures that enable expeditious and effective collaboration during investigations.
- Cooperation in conducting police investigations and obtaining testimony for use in judicial proceedings, giving consideration also to the use of information and communications technologies.
- The development of guidelines, standards, methodologies and best practices for the prevention and investigation of cybercrime offences.
- The fostering of collaboration between national computer emergency response teams or computer security incident response teams in preventing cybercrime.
- Coordinated investigations.
- Recommend a minimum common framework for transparency and the protection of information so that, regardless of the differing national policies of each State, data from investigations and judicial proceedings can be shared.
- Establish minimum time limits for retaining data and preserving digital evidence.

- Recommend rules and conditions to which the interception of private communications and real-time geolocation should be subject.
- Establish general parameters for compliance with and regulation of privacy policies.
- Promote the harmonization of local, regional and global statistics.

Aspects relating to the protection and exercise of human rights

All measures to be implemented under the future convention should be consistent with the obligations set out in international human rights instruments. Its provisions are also expected to be compatible with standards relating to freedom of expression.

The Government of Mexico hopes that the following will be addressed in the course of elaboration of the convention:

- Concepts and developments relating to business and human rights.
- Emphasis on the investigation, prosecution and punishment of gender-based violence and offences against children and adolescents through the Internet.
- Encouragement of the investigation, prosecution and punishment of racist conduct that incites violence or is aimed at causing exclusion or segregation.
- Minimum common elements of network neutrality.
- The recommendation of mechanisms for the protection of information by Internet service companies.

Elements relating to capacity-building and technical assistance

The Government of Mexico considers that, in order for the future convention to be implemented effectively, it will be necessary to establish provisions that promote capacity-building with respect to both the prevention and the prosecution of cybercrime offences. It would be desirable:

- To encourage efforts in relation to training, technical assistance and best practices, as well as standardized procedures for conducting computer forensics and obtaining valid digital evidence.
- To promote prevention-oriented education initiatives and replicable public awareness campaigns.
- To encourage also the establishment or strengthening of computer emergency response teams in various sectors, such as finance, education, trade and energy.
- To develop guides, guidelines and recommendations that promote the adoption of best practices.
- To expand the range of training activities aimed at different stakeholders: investigators, prosecutors, judges, diplomats, legislators and non-State actors.

Aspects relating to the participation of relevant non-State actors (civil society, private sector, academia)

The Government of Mexico considers it advisable to explore through the drafting process mechanisms for facilitating the participation of, and the provision of inputs by, civil society organizations, the private sector, service providers, academia and research centres. It would be desirable to consider the following:

- The possible involvement of those actors in processes aimed at preventing and countering cybercrime.
- The promotion of collaborative environments with private computer emergency response teams, carriers and various telecommunications companies.

- Dialogue with private enterprises operating critical information infrastructure or working in strategic sectors, and with companies providing cost-free Internet services such as email, instant messaging, microblogs and online transport services.
- Support for self-regulation and social awareness and promotion of the concept of business and human rights.

New Zealand

[Original: English]
[29 October 2021]

New Zealand is pleased to respond to the invitation from the Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes to Member States to submit their views on the scope, objectives and structure of the new convention, with regard to the implementation of General Assembly resolutions 74/247 and 75/282. New Zealand welcomes the opportunity to share its views and looks forward to the contributions of others and to discussing a path forward as we work together in a transparent, inclusive manner to elaborate a new convention.

Cybercrime is a transboundary challenge. It follows that global cooperation rooted in an inclusive and multi-stakeholder approach is the only way to ensure that the international community is able to effectively counter this growing threat. International cooperation on cybercrime-related issues requires consistent, effective cybercrime laws that enable investigation and prosecution of cybercrime across borders. Facilitating this cooperation has never been more important. As work, research and social interactions have shifted online, including over the course of the coronavirus disease (COVID-19) pandemic, the areas of opportunity for cybercriminals have broadened and we have seen cybercrime incidents increase in both frequency and severity.

International cooperation on cybercrime is particularly essential for small island developing States and it is imperative that these countries are able to engage meaningfully in the work of the Ad Hoc Committee. New Zealand is committed to ensuring that Pacific island countries are able to meaningfully participate in the work of the Ad Hoc Committee. We support hybrid (in person and online) participation for sessions of the Ad Hoc Committee and emphasize the importance of allowing time for adequate preparation and participation by smaller delegations.

Scope

The new cybercrime convention must complement rather than conflict with existing instruments. All Member States have agreed that international law applies to cyberspace, which means that this new convention will not exist in a vacuum. It will be most effective if it complements and reinforces existing instruments and the current legal regime, which includes tools to address cybercrime such as the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime. This is in line with the mandate provided by General Assembly resolution 74/247, in which the Assembly called for the work of the Ad Hoc Committee to take into full consideration existing international instruments and efforts at the national, regional and international levels.

For New Zealand, it is essential that any instrument that is developed protects human rights and upholds a cyberspace that is governed by multiple stakeholders, free and open. The cybercrime convention must therefore be consistent with States' obligations to protect and respect human rights online, including the right to freedom of expression and the right not to be subjected to arbitrary and unlawful interference

with privacy. Measures to combat cybercrime must be consistent with international human rights law.

The treaty should be sharply focused on core cybercrime issues in order to effectively strengthen cooperation to tackle the threat these pose to individuals, industry and governments. We consider that the treaty should cover cyber-dependent offences, together with cyber-enabled crimes, only where the scope, speed and scale of the offence is increased by use of information and communications technologies. We consider that there are two clear candidates for this category of crime: child sexual exploitation and abuse online, and cyber-enabled fraud and theft, including ransomware.

New Zealand does not consider that there is a need to duplicate offences that are covered by other legal instruments, such as corruption, trafficking or terrorism, simply because these may be carried out using information and communications technologies. Such an approach risks contradiction and confusion and will not deliver a targeted, practical instrument that can improve our collective ability to tackle cybercrime.

The mandate for this process clearly articulates that we should focus on developing a criminal justice instrument to improve the international response to cybercrime, through actions taken by national law enforcement agencies. This requires defining and sanctioning criminal conduct in cyberspace and for States to implement appropriate processes and legislative tools that enable agencies to access and share digital evidence to effectively disrupt and place sanctions on criminal conduct in cyberspace. It does not require defining norms for non-criminal behaviour online. We consider that there is value in learning from other criminal justice treaties that have been successful where they have focused on core criminal issues, alongside broad international cooperation provisions and support to build capacity in all Member States.

The language of an eventual convention must be practical, technologically neutral and future-proofed to the extent possible in order to ensure that it stands the test of time and does not require constant revision. This means that we will need to focus on the activity rather than on the particular form or method used to carry out that activity.

It would be premature at this stage to determine what may be required in terms of an implementation mechanism for a convention. There are a wide range of models to consider, but this aspect of the treaty can be set aside until the scope of the instrument and its objectives are more clearly defined.

Objectives

The primary purpose of the new instrument should be a harmonized, modern and effective global framework for cooperation and coordination between States to tackle the growing threat posed by cybercrime to individuals, business, critical infrastructure and governments. It should include the provision of support and technical assistance to enable all States to develop the capacity and capability to respond to these challenges. This will increase the ability of States to respond effectively to cybercrime nationally, regionally and internationally.

This means that the treaty needs to support cooperation between national law enforcement, prosecution and judicial agencies bilaterally or multilaterally in preventing, investigating and prosecuting the offences set out in the treaty. This is critical to combating cybercrime, given that, owing to its transboundary nature, cybercrime often involves perpetrators and victims based in multiple jurisdictions. A common understanding of what constitutes criminal offences in the context of cyberspace and which offences should be punishable in domestic jurisdictions will help facilitate this, particularly if complemented by consistent frameworks for accessing and sharing digital evidence with international partners, with appropriate safeguards.

The use of powers to investigate and prosecute offences set out in the treaty must be subject to effective safeguards in relation to human rights and fundamental freedoms, as set out in existing international treaties. Safeguards must also exist to ensure that mutual cooperation powers are used fairly and appropriately and allow States to refuse cooperation when certain standards are not met. In addition, New Zealand considers that the treaty must recognize the independence of national law enforcement and prosecutorial agencies, and that the decision on whether to take action lies solely with those agencies in the respective Member States.

Effective international cooperation is best achieved through a widely supported treaty. New Zealand considers that this requires the treaty negotiations to be inclusive and transparent, with best endeavours made to reach consensus, so as to secure the strongest possible mandate for the convention. All Member States should be able to share their views and engage meaningfully in negotiations supported by the expertise and perspectives of civil society, industry and other relevant stakeholders. The perspective of indigenous peoples, including Maori in Aotearoa New Zealand, as well as other minority groups, should be included, along with the potential impact of cybercrime and efforts to combat it on such groups.

International cooperation to combat cybercrime is not as effective as it could be. This is not due to a lack of will from Member States, but rather a lack of capacity or expertise. Technical assistance and capacity-building for law enforcement institutions is a critical requirement and the convention needs to support the development of capacity and capability globally.

Structure

We look forward to hearing the views of other States in relation to the scope and objectives of the convention through this process and at the first negotiating session in January 2022. Following this, we anticipate that a clear path forward in terms of structure will emerge rapidly.

Nigeria

[Original: English]
[5 November 2021]

Nigeria believes that to effectively respond to the fast-evolving threats of cybercrime, there is an urgent need to define and place sanctions on criminal conduct in cyberspace, improve synergy in transnational policing capabilities, improve procedural tools and reform and/or enhance international cooperation, while respecting human rights. Thus, the elaboration of a United Nations convention on the subject matter must at this time focus on the fight against cybercrime and not attempt to cover cybersecurity and other cyber-related matters that are politically volatile and better addressed in other United Nations forums. It is imperative that the negotiation of the new convention be a transparent, inclusive and consensus-driven process, one that engenders wider acceptability and/or adoption of the resultant convention.

Scope

The new cybercrime convention should create a legal and institutional framework to counter cybercrime that includes the following elements:

(a) The criminalization of substantive cybercrime offences: define and provide sanctions for cyber-dependent crimes, which are crimes in which computers or data are the targets of the criminal activity, and certain cyber-enabled crimes, as well as the laundering of proceeds of cybercrime;

(b) The provision of procedural powers for the investigation and prosecution of established cybercrime offences, as well as for obtaining and sharing electronic evidence of other criminal offences;

(c) Provisions or measures for sustainable capacity-building and technical assistance;

(d) Provisions or measures for the recovery of the proceeds of cybercrime, and restitution;

(e) Provisions or measures for improved collaboration and coordination between law enforcement agencies and the private sector;

(f) Provisions or measures for enhanced international cooperation in relation to the above matters, including direct cooperation with Internet service providers; and

(g) Provisions or measures to prevent cybercrime and increase awareness, including working with civil society organizations, the private sector, service providers, academia and research centres.

Objectives

The new convention should aim at the following objectives:

(a) A common understanding of established baselines for substantive cybercrime offences, procedural powers and international cooperation to fight cybercrime;

(b) Promote the criminalization of offences in a technologically neutral manner to ensure that the substantive criminal provisions address not only present-day technologies and criminal techniques, but also future technologies and techniques;

(c) Establish authorities and capabilities to collect, obtain and share electronic evidence of cybercrimes and other offences, consistent with due process and the protection of human rights and fundamental freedoms;

(d) Promote and facilitate international cooperation in the fight against cybercrime and eliminate safe havens for cybercrime perpetrators;

(e) Promote capacity-building and technical assistance to strengthen the capacity of law enforcement authorities to address cybercrime, as well as the use of existing institutional capacities such as International Criminal Police Organization (INTERPOL) databases;

(f) Promote the utilization by Member States of multilateral instruments that have already proved their usefulness in the fight against cybercrime, such as the Council of Europe Convention on Cybercrime, and the nexus with existing United Nations treaties in the field of crime prevention and criminal justice, in particular the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption;

(g) Promote practitioner-level intergovernmental and multi-stakeholder processes for trusted information-sharing to identify future cybercrime trends, threats and mitigation measures; and

(h) Establish a mechanism to monitor and/or facilitate the effective use and implementation of the convention, exchanges of information and the consideration of any reviews and/or future amendments.

Structure

In addition to the preamble, clear definitions and appropriate final provisions, it is considered important that the following elements form part of the structure of the new convention:

(a) General provisions and/or objectives and their application;

(b) Cybercrime prevention measures, similar to those found in the Organized Crime Convention and the Convention against Corruption, for instance, provisions on awareness-raising and educational initiatives;

(c) Substantive cybercrime offences and penalties;

(d) Procedural law provisions and general investigative powers;

(e) Safeguards to ensure that law enforcement activities comply with international human rights;

(f) International cooperation in combating cybercrime, including both formal and informal international cooperation for the detection, investigation and prosecution of cybercrime, as well for obtaining electronic evidence of other criminal offences;

(g) Provisions for capacity-building and technical assistance to enhance the skills of practitioners and strengthen the capacity to address cybercrime;

(h) Provisions for practitioner-level multi-stakeholder collaboration for the trusted sharing of information and experiences with relevant stakeholders;

(i) Provisions for an established mechanism to monitor and/or facilitate the effective use and implementation of the convention, the exchange of information and the consideration of any reviews and/or future amendments.

Norway

[Original: English]
[3 November 2021]

The Government of the Kingdom of Norway is pleased to respond to the invitation to Member States to submit their views on the scope, objectives and structure of the new convention on countering the use of information and communications technologies for criminal purposes, with regard to implementation of General Assembly resolutions 74/247 and 75/282. International cooperation is key to tackling the continuously developing threats of cybercrime, and the Government of Norway looks forward to participating in the negotiations for a comprehensive convention on the matter.

Scope

In its resolution 74/247, the General Assembly decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. As the resolution clearly targets criminal behaviour, criminalization of core cybercrime offences should be a central part of the convention.

Questions regarding cybersecurity and cybergovernance fall outside the mandate given by the General Assembly and should not be the topic of the convention. These matters are subject to other United Nations forums and processes. Attempts to include provisions on cybersecurity and cybergovernance will make it harder to create an instrument that will attract broad support.

Cybercrime has already been a challenge for decades, and it is a persistent problem that criminal perpetrators are often one step ahead of national law enforcement agencies. Cybercrime tomorrow is not the same as cybercrime today, and the ongoing digital revolution has created an immense task for the international community of States. In that regard, it is of utmost importance to strive for the inclusion of an updated and modern catalogue of offences that can stand the test of time.

Even though cybercrime is developing every day, national and international agencies have managed to identify central, reoccurring types of conduct. These offences are already criminalized in many Member States today. In that regard, the

Government of the Kingdom of Norway would like to recommend that at least the following cyber-dependent and cyber-enabled offences be considered:

(a) Illegal access, that is, accessing a computer or computer system without authorization;

(b) Illegal interception, that is, the real-time unlawful interception of the content of communications or traffic data related to communications;

(c) Data or system interference, that is, malware, denial-of-service attacks, ransomware, and data deletion or modification;

(d) The misuse of devices, that is, trafficking in or using credit data, passwords and personal information that permit access to resources;

(e) Offences related to child sexual abuse materials;

(f) Offences related to computer-facilitated fraud, that is, manipulation of computer systems or data for fraudulent purposes such as phishing, the compromising of business emails and auction fraud;

(g) Offences related to infringement of copyright and related rights.

The convention should also include provisions on attempt, aiding and abetting and conspiracy, the laundering of the proceeds of cybercrime, and the liability of corporations and other legal persons.

Since cybercrime is developing continuously, it is important for the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes to focus on updated reports from national law enforcement agencies and equivalent reports from regional and international organizations. The United Nations Office on Drugs and Crime Comprehensive Study on Cybercrime is important. The Government of the Kingdom of Norway would also like to call attention to the annual Internet Organised Crime Threat Assessment of the European Union Agency for Law Enforcement Cooperation (Europol), as a significant source of information regarding dominate types of cybercrime.

In addition to provisions on criminalization, the convention should also include provisions on procedural authority, in particular provisions on the collection and sharing of electronic evidence. It is important that these provisions are consistent with due process and the protection of human rights and fundamental freedoms.

Dealing with the challenge of modern cybercrime, the convention should require Member States to include domestic provisions specifically aimed at electronic evidence, such as rules on expedited preservation of stored computer data, search and seizure of stored computer data and real-time collection of computer traffic data and content data in cases of serious crime. Furthermore, the convention should allow cooperation to collect and obtain electronic evidence for any type of crime, not only cybercrime.

In particular, the Ad Hoc Committee should consider provisions on obtaining electronic evidence in the so-called “cloud”. In the last decade, storage of computer data in the cloud has been a recurring challenge for national law enforcement agencies, owing in particular to jurisdiction-related issues and the dependency on other States. A modern and updated convention on cybercrime should therefore reflect how Member States can cooperate to secure evidence stored by means of the cloud in other States.

It is also necessary for the convention to include provisions on international cooperation. In this regard, the Ad Hoc Committee should draw on experiences from existing treaties, especially the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption. Provisions on extradition and mutual assistance should be taken into account.

It is also important for the convention to reflect the different abilities of Member States to comply with the suggested provisions, in particular those regarding technical infrastructure and capabilities. Therefore, the convention should establish instruments for capacity-building and provide avenues for Member States to seek such assistance.

Finally, the convention should address how citizens, businesses, organizations and other stakeholders can work together with governments to protect themselves and the community from cybercrime. Even though cybersecurity falls outside the scope of the convention, prevention of cybercrime is naturally relevant, and should be considered.

Objectives

The Ad Hoc Committee should aim to create a robust convention that requires the Member States to adopt national legislation that improves the prevention and handling of cybercrime globally. Domestic provisions on criminalization of certain types of cybercrime, as well as provisions on procedural authority and international cooperation, will be especially important.

It should be an objective for the upcoming drafting process to create an instrument that can stand the test of time and that is up to date with all modern forms of cybercrime, as well as the most likely trends to come. Furthermore, it should be an objective to draft an ambitious instrument that can adequately address the central cybercrime challenges. At the same time, a consensus-based approach is vital.

The Government of the Kingdom of Norway would also like to reiterate the importance of maintaining an open, inclusive, transparent and multi-stakeholder process that will allow all Member States to negotiate in good faith toward well-informed, practical solutions, which we believe is key to ensuring widespread accession to the new convention.

Structure

Taking into account the proposed scope and objectives of the convention, the main parts of the convention are a given. However, it will be fruitful for the Ad Hoc Committee and the Member States to have an open mind regarding the structure of the convention. Even though provisions on criminalization, procedural authority and international cooperation should make up central parts of the convention, other matters may also influence the final structure. The Government of the Kingdom of Norway recommends an open approach to the structure of the convention.

Human rights

International human rights law applies to cyberactivities just as it does to any other activity. States must comply with their human rights obligations in cyberspace just as they must in the physical world. States must both respect and protect human rights, including the right to freedom of expression and the right to privacy, and other relevant data protection principles.

It is self-explanatory that human rights standards as enshrined in the International Covenant on Civil and Political Rights entail an important framework for any new provisions on cybercrime. Regardless, the Government of the Kingdom of Norway would like to reiterate the importance of human rights in the upcoming negotiations, especially regarding provisions requiring national legislation on procedural authority.

Oman

[Original: Arabic]
[18 October 2021]

The targeting of civilian facilities, especially vital infrastructure facilities – including electricity and water networks, financial institutions and the transport sector – should be criminalized. Such facilities should not be transformed into arenas for conflict between countries and for the settling of accounts.

Panama

[Original: Spanish]
[28 October 2021]

The constant evolution of technology makes it necessary for States to adopt mechanisms to prevent and combat new forms of crime. The COVID-19 pandemic has exacerbated a problem that was already becoming increasingly evident: we are not sufficiently prepared for combating cybercrime and offences that are committed through technological means.

Being prepared for that battle requires, among other things, awareness that the investigation of cybercrime and offences committed through digital means cannot be dissociated from the international dimension of the topic. All States are affected by the criminal activities of those who find in transnationalism fertile ground for achieving their goals and avoiding liability.

In the light of the above considerations, the comprehensive international convention on countering the use of information and communications technologies for criminal purposes should serve as a tool for facilitating the investigation by States of such offences. To that end, it is important that the convention cover not only acts that directly affect information, computer systems and technology itself but also those that are committed through technological means, regardless of the legally protected right concerned.

We believe that this new tool should establish measures to improve systems for formal and informal communication between States so as to achieve more effective investigations, given the volatility of information.

In line with a strengthened communication system, legal concepts delimiting such investigative measures as the seizure of data and correspondence, the preservation of data and the handling of electronic evidence should be addressed.

While we are aware that there may be conflicting positions on certain issues, the objective remains the same: to create an instrument that contributes to countering the use of information and communications technologies for criminal purposes.

Russian Federation

Note by the Secretariat: the submission by the Russian Federation is contained in document A/75/980, entitled “Letter dated 30 July 2021 from the chargé d’affaires a.i. of the Russian Federation to the United Nations addressed to the Secretary-General” and in the annex to that letter, entitled “Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes”, which was made available to the General Assembly at its seventy-fifth session. It is being transmitted to the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes as part of the submission of views from Member States on the scope, objectives and structure (elements) of the new convention, as per the invitation of the Chair of the Ad Hoc Committee.

Switzerland

[Original: English]
[28 October 2021]

Information and communications technologies (ICTs) have had a deep impact on our society, offering opportunities for development at the social, cultural and economic levels, but also providing a basis for activities with criminal purposes that take place in cyberspace. As our world becomes increasingly digitalized, cybercrime is on the rise. Through its resolution 74/247, the General Assembly established an open-ended ad hoc intergovernmental committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. The present reply outlines the view of Switzerland on the objectives, scope and structure of this instrument.

Objectives

For Switzerland, the overarching goal of a United Nations convention on countering the use of ICTs for criminal purposes is to protect ICT users, so that they can use ICTs freely and enjoy their benefits. The global and open nature of ICTs is indeed a driving force in accelerating progress towards social and economic development. The aim of the convention is therefore the safety of users, which should not hamper their freedom to use ICTs. Users must be able to exercise their human rights and fundamental freedoms online, thereby realizing the full potential of an inclusive digitized world. The convention should therefore be a step further in ensuring free, trusted and safe ICTs.

A United Nations convention can help us attain this overarching goal. To do so, the convention should provide for a coordinated approach in the fight against cybercrime. Because of the inherently transnational nature of ICTs, cybercrimes are likely to involve perpetrators and victims based in multiple States. International cooperation is therefore key to ensuring the best level of protection against cybercrimes. The convention should be aimed at creating a common understanding of what constitutes criminal offences in the context of ICTs, and which offences should be punishable under national law. This common understanding is the first building block for enabling any sort of cooperation. On the basis of this shared understanding and vocabulary, the convention should be aimed at creating the framework for effective international cooperation to protect ICT users and obtain justice for the victims of cybercrime.

A coordinated approach to fighting cybercrime at the global level can only be achieved through an inclusive process. All Member States should be able to engage meaningfully; they should have the opportunity to present their views on the convention and to discuss the views presented by others during the substantive meetings of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. The Ad Hoc Committee should strive for consensus, whenever possible.

Cybercrime is transnational, but also inherently involves non-State actors. If we want a convention that is fit for purpose, every voice needs to be heard during the elaboration process. Including all stakeholders, among which are relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, in each coordinated step of the elaboration is key to ensuring that the convention can fulfil its objectives.[8]

Scope

International law applies to cyberspace. The future convention will not exist in a vacuum, nor will it empty previous international agreements of their significance.

[8] In accordance with General Assembly resolution 75/282, paragraphs 9–10.

It is the conviction of Switzerland that this convention must build upon and should reinforce the current legal regime. It should be designed to complement the initiatives already undertaken by the international community, and to rely on synergies to effectively tackle cybercrime.

As the convention will be a criminal law treaty, it should build upon and respect international criminal law. Global tools to address the issue of cybercriminality already exist. Along with the United Nations Convention against Transnational Organized Crime, the Council of Europe Convention on Cybercrime has been a standard by which countries around the globe, including Switzerland, have been modernizing their cybercrime laws. It is also an important baseline for international cooperation in the Internet age. A United Nations convention should build upon this experience. The work of the Ad Hoc Committee should be guided by the work of other groups and forums, including the Expert Group to Conduct a Comprehensive Study on Cybercrime.

The convention must adequately reflect, safeguard and reinforce human rights law. As cybercrime poses a threat to the human rights of individuals, efforts to address it need to protect, not undermine, these rights. The same rights that individuals have offline must also be protected online. Measures undertaken to combat cybercrime must be consistent with international human rights law.

Structure

Switzerland considers that a promising and efficient approach to concretize the objectives mentioned above is to follow the structure of existing international criminal law instruments negotiated in the context of the United Nations. The convention could therefore be structured as follows:

(a) General provisions;

(b) Preventive measures;

(c) Criminalization and law enforcement;

(d) International cooperation;

(e) Technical assistance and information exchange;

(f) Mechanisms for implementation;

(g) Final provisions.

Switzerland considers that there is no need to duplicate offences that are already covered by specific treaties (for example, corruption, trafficking and terrorism) simply for the reason that they may (also) be committed by means of ICTs. Instead, the convention should focus on crimes that are specific to cyberspace. A broad listing of offences, even if they all may be committed by means of computer systems, entails the risk of contradiction and should be avoided.

Content-related offences should be kept to a minimum and should always be evaluated with regard to their added value.

Switzerland emphasizes the need for and importance of procedural guarantees that ensure the legality and fairness of proceedings and the rights of the persons affected, in particular with regard to mutual legal assistance, the exchange of information and extradition under the conditions set by the concerned States. The right to privacy must be fully guaranteed. An adequate level regarding the protection of personal data must be ensured.

Adequate conditions and safeguards must be considered and introduced, in particular with regard to maintaining and strengthening human rights, including the principle of non-discrimination.

Turkey

[Original: English]
[4 November 2021]

Turkey attaches utmost importance to free, open and secure use of information and communications technologies around the world.

The development of information and communications technologies enhances the risk of misuse of these technologies for criminal purposes. Eliminating these risks and threats to the security of critical infrastructure facilities and to fundamental rights and freedoms should be one of the top priorities of the international agenda. Owing to the transnational nature of cyberspace, the impact of attacks in this field can reach up to the global level. Reducing the impact of these attacks is possible only with effective cooperation carried out at the global level.

In this regard, Turkey attaches utmost importance to effective international cooperation for a more stable and secure cyberspace at the global level. In this respect, Turkey is ready to contribute to and support the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. In this context, we would like to share our initial views on the scope, objectives and structure of the convention.

The following issues need to be considered in the context of the convention:

(a) The development of effective cooperation channels among States;

(b) The clear definition of matters related to the criminal use of information and communications technologies;

(c) The development of emergency communication channels among States;

(d) Improving resources for the gathering and acquisition of intelligence on cyberthreats;

(e) The development of intelligence-sharing among the relevant institutions of States;

(f) Information-sharing in cases involving the criminal use of information and communications technologies.

In addition, effective measures to prevent the internal communication of criminals and terrorists and their propaganda activities should be included in the convention.

The coronavirus disease (COVID-19) pandemic has significantly increased the use of remote telecommunication; therefore, during the negotiations for the convention, we should also consider the effects of the pandemic on the criminal use of information and communications technologies.

In addition, it will be beneficial to consider within the scope of the convention the safe use of new-generation technologies such as cloud computing, 5G, blockchain, the Internet of things and artificial intelligence in the fight against crime and cyberattacks.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[28 October 2021]

Scope

The United Kingdom believes that the new international cybercrime convention should focus on strengthening cooperation to tackle the growing threat posed by criminal activity to citizens, businesses and governments.

There are a number of existing regional and international cybercrime treaties that have already contributed significantly to efforts to tackle cybercrime. It is important to both build on the success of such treaties and to recognize the relevant provisions of criminal justice treaties such as the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime.

The scope of the treaty should include: (a) the investigation and prosecution of the offences defined in the treaty; (b) the development of capacity and capability to enable all Member States to tackle these offences; and (c) the recognition of an expert forum through which new and emerging threats can be identified.

The United Nations treaty on cybercrime should cover cyber-dependent offences, together with cyber-enabled crimes, where the scale, scope and speed of the offence is increased by the use of a computer. Cooperation is effective where the offences included in the treaty are commonly understood and recognized by all legal systems.

The offences in the treaty should not undermine the exercise of freedom of expression or opinion.

This is a criminal law treaty and should therefore focus on the activity to be undertaken by national administrations. It should also consider how, through a multi-stakeholder approach, citizens, non-governmental organizations, civil society organizations, academic institutions and the private sector can work together to protect themselves from cybercrime.

Any treaty must contain strong safeguards that include respect for privacy and other human rights, as set out in international human rights law and recognized in relevant resolutions adopted by the General Assembly and the Human Rights Council.

The treaty must be developed in an inclusive and transparent manner, respecting the views of all Member States and with the active participation of a wide range of stakeholders, including non-governmental organizations, civil society organizations, academic institutions and the private sector. Furthermore, the treaty's provisions, for example, those on implementation and capacity-building, should also encourage an inclusive and transparent approach to tackling cybercrime.

The language should be technologically neutral to ensure that the treaty stands the test of time and does not require constant updating.

The treaty should not replicate work that has already been done or that should properly be done elsewhere. The treaty should not extend to matters of cybersecurity, which are already addressed by the First Committee of the General Assembly, or matters of Internet governance, which are already addressed in dedicated multi-stakeholder forums.

Objectives

The primary purpose of the treaty should be to support the effective cooperation of national law enforcement and prosecutorial agencies, bilaterally or multilaterally, in investigating and prosecuting the offences set out in the treaty. A treaty that is widely supported will enable the widest possible international cooperation.

To support effective mutual cooperation, there must be options for refusal on the grounds of dual criminality, refusal in respect of political offences, particularly where the alleged offence relates to the exercise of freedom of expression, and refusal of a request made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender or other protected characteristics. It would be useful to have minimum standards that the requesting authority must confirm they have met, such as the request being necessary, proportionate, time-limited and authorized at a specific level.

The use of powers to investigate and prosecute offences set out in the treaty, including those used in bilateral or multilateral cases, must be subject to effective safeguards in relation to human rights and fundamental freedoms, as set out in international human rights law.

The treaty must recognize the operational independence of national investigative and prosecutorial agencies, and that the decision on whether to take action lies solely with those agencies.

The treaty should support the development of capability globally, and support capacity-building.

The threats from criminal activity in cyberspace will change, and the treaty should determine an intergovernmental and multi-stakeholder process to identify future threats, without prejudice to whether that process forms part of the treaty.

Given that different genders are affected in different ways by cybercrime, the treaty should be gender-inclusive in order to help us tackle cybercrime more effectively. Developing a cybercrime treaty that is cognizant of the gendered implications of its provisions will encourage more women to participate at all levels and in all processes. This will result in more diverse, richer and ultimately better solutions. At the meeting of the intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime in April 2021, all Member States agreed that they should promote, in particular, the participation of women experts.

The treaty should promote a “whole of society” approach to tackling cybercrime and encourage Member States to work together with actors outside of government, including experts, industry and the general public, on areas such as raising awareness, improving education, gender and cybercrime training, and victim support.

Structure

The United Kingdom believes that the following structure would be an effective means of organizing the treaty:

(a) General provisions

The general provisions should include the basis and purpose of the treaty, and the definitions that will be used throughout the treaty. The definitions must be commonly understood and agreed by all parties, and must be technologically neutral, taking into consideration terminology that has been widely agreed upon in regional instruments and used in national legal frameworks;

(b) Core offences

The offences must include cyber-dependent offences (e.g. illegal access), with descriptions and definitions that are acceptable to all parties. Cyber-enabled offences (e.g. child sexual exploitation and abuse, or fraud) should be included where the offence is mainly carried out online, where computers change the scale and speed of the offence and where the definitions of the offence are commonly understood;

(c) Human rights and safeguards

The operation and implementation of the treaty must be underpinned by meaningful procedural safeguards and strong protections for human rights, and reference international human rights law;

(d) Preventive measures

As with the Convention against Corruption and the Organized Crime Convention, the treaty should include provisions encouraging States to implement measures to prevent cybercrime, including through working with all relevant stakeholders;

(e) Procedural law provisions

The powers to support investigations and prosecutions must allow appropriate authorities to preserve, search and seize electronic evidence for any offence committed by means of a computer or where the evidence relating to an offence is in electronic form, for both domestic and international investigations;

(f) International cooperation

The international cooperation provisions must cover mutual legal assistance and assistance in an emergency, including a requirement for countries to set up 24/7 contact points. Alongside the practical sharing of evidence, the recommendations made by the Expert Group in April 2021 made clear that Member States want to continue to share experiences and best practices, as well as information on new and growing threats;

(g) Technical assistance and capacity-building

Capacity-building should be encouraged, with a significant role for the United Nations Office on Drugs and Crime, and there should be coordination of such work through existing structures such as the Global Forum on Cyber Expertise. The United Kingdom notes the large number of recommendations agreed by the Expert Group in April 2021 that focused on capacity-building, including the provision of specialist and up-to-date training for practitioners on cybercrime investigations, the handling of electronic evidence, chain of custody and forensic analysis;

(h) Implementation

There should be a clear plan for implementation of the treaty.

United States of America

[Original: English]
[28 October 2021]

The Government of the United States of America is pleased to respond to the invitation to Member States to submit their views on the scope, objectives and structure (elements) of the new convention, with regard to the implementation of General Assembly resolutions 74/247 and 75/282. The United States looks forward to working together with other Member States and interested stakeholders to draft a global instrument focused on improving the investigation and prosecution of cybercrime, consistent with and building upon existing rights and obligations. The United States reiterates the importance of maintaining an open, inclusive, transparent and multi-stakeholder process that will allow all Member States to negotiate in good faith towards well-informed, consensus-based, practical solutions, which we believe will encourage widespread accession to a new global anti-cybercrime instrument.

The proposed deadline for our work would create a tight timeline even in ordinary circumstances, but our present efforts will be undertaken against the backdrop of a global pandemic. Therefore, it is all the more essential to be focused and efficient in our efforts to negotiate towards a global anti-cybercrime instrument. Unfortunately, while most of the world has worked to combat the coronavirus disease (COVID-19) pandemic, cybercriminals have exploited the resulting global shift and reliance on digital technologies. Cybercrime is a direct threat to the safety and well-being of societies and people around the world. There has been long-standing cooperation to build our collective capacity to combat this exploitation, and we can continue to build on those successes with careful consideration of practical solutions. Given the immediacy of the cybercrime threat, it is therefore all the more essential to be focused and deliberate in our efforts to negotiate a global anti-cybercrime instrument.

This anti-cybercrime instrument should be aimed at enhancing international cooperation and providing practical tools to equip national law enforcement authorities to tackle cybercrime, as other United Nations instruments have done for

other forms of transnational crime, including corruption, narcotics trafficking, human trafficking and migrant smuggling. The instrument should also ensure domestic authority to collect and obtain electronic evidence relevant to any type of crime, not only cyber-dependent crime, and promote international cooperation in such cases. As with every United Nations anti-crime instrument, these tools should include appropriate limits and safeguards, in the context of existing domestic frameworks, to address privacy and civil liberties, while fully respecting human rights. The anti-cybercrime instrument should also address the growing need for technical assistance and provide avenues for Member States to seek such assistance.

As Member States begin the drafting process, it is essential to recognize that we do not do so in a vacuum. As important as it is to define what this instrument should cover, it is equally important to recognize what lies outside its proper scope. Valuable ongoing work on other cyber-related issues beyond the scope of cybercrime is being conducted in the United Nations and other intergovernmental and multi-stakeholder forums. It is important that we do not duplicate or undermine that work, both to avoid conflicts of obligations and so as not to detract from our objective to produce a targeted, practical instrument to fight cybercrime. Attempting to address every cyber-related issue in this criminal justice instrument risks miring these negotiations in unfocused and tangential debates that would do little to combat cybercrime and only slow our progress towards a useful instrument.

In particular, Member States should not delve into wide-ranging cybergovernance or cybersecurity topics in a crime instrument dedicated to combating cybercrime. Although often seen as two sides of the same coin, cybercrime enforcement is essentially a governmental responsibility, whereas cybersecurity is the responsibility of a range of public and private actors. The mandate of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is focused on developing a criminal justice instrument on criminal matters to facilitate an international response to cybercrime, which involves defining and providing sanctions for criminal conduct in cyberspace. The Ad Hoc Committee is not empowered to dictate global norms for non-criminal behaviour online. Including cybergovernance and cybersecurity concepts in a cybercrime treaty would not meet the objective of a streamlined and effective instrument that will attract broad support from Member States.

As reaffirmed in General Assembly resolution 75/282, it is vital that negotiations towards a new anti-cybercrime instrument do not impede existing mechanisms, including multinational and regional instruments that already provide an array of tools to effectively combat cybercrime. We can best build consensus for this new instrument and avoid political and divisive issues by drawing from existing instruments that have proved successful. We should be guided by the achievements in implementing other United Nations criminal justice treaties, such as the United Nations Convention against Transnational Organized Crime. The Organized Crime Convention has proved to be extremely useful because the instrument is targeted at core types of organized crime activity, while also including broad international cooperation provisions that may be applied to any type of serious crime committed for profit by three or more persons. As a result, the parties have used the Organized Crime Convention successfully thousands of times, including to combat crimes, such as ransomware incidents and child sexual exploitation.

The United States again reiterates the importance of maintaining an open, inclusive and transparent process that will allow all Member States and interested stakeholders to negotiate in good faith towards well-informed, consensus-based, practical solutions, which we believe is the best way to encourage widespread accession to a new global anti-cybercrime instrument.

Criminalization of core cybercrime offences

First and foremost, any new instrument should ensure domestic authority to collect and obtain electronic evidence for any type of crime. Such authority is imperative for countries to be able to effectively investigate and prosecute almost every type of crime, as very few present-day crimes are completely conducted outside the digital realm. The instrument should also enable international cooperation for the sharing of electronic evidence of any type of crime, subject to a flexible dual criminality provision as contained in the Organized Crime Convention and the United Nations Convention against Corruption.[9]

In addition, effective international cooperation requires Member States to have adequate domestic legislation that criminalizes core cybercrime offences. A shared understanding of core substantive offences and supporting procedural authority among Member States is essential to avoid creating safe havens for cybercriminals. Studies by the United Nations Office on Drugs and Crime (UNODC) show that countries generally agree on core conduct that should be criminalized by specific cybercrime statutes, with many multinational agreements and national criminal statutes containing common provisions. Similarly, international understanding of lawful types of procedural authority to support effective cybercrime investigations is settled. As a result, practitioners have two decades of accumulated and varied experience in investigating cybercrime that demonstrates the continuing viability of commonly adopted types of substantive and procedural authority to investigate cybercrime.

A new anti-cybercrime instrument should define and apply to cyber-dependent crimes, which are crimes in which computers or data are the targets of the criminal activity, as well as certain cyber-enabled crimes, that is, crimes in which a computer is used to facilitate the crime. This first and principal category of offences to be defined in this new instrument comprises those that cannot be committed without the misuse of computers or network systems and that therefore did not exist as crimes prior to the advent of computer systems. Cyber-dependent crimes can take place completely in the digital realm. For core cyber-dependent criminal offences, such as denial-of-service attacks or damage to computers and data, cyber-specific statutes are needed because, in most jurisdictions, criminal laws are construed strictly, and traditional laws that cover familiar concepts, such as trespass and vandalism, are often inadequate to apply to cybercrime. Moreover, certain criminal code provisions that are applicable to crimes committed outside a computer network may not be easily applied to conduct committed by means of computers.

In contrast, we should be careful not to treat traditional crimes as “cybercrime” merely because a computer was involved in their planning or execution. Despite the misuse of a computer to commit the crime, some culpable conduct may be covered by general statutes because there is nothing peculiar or unique to using a computer system in that conduct. In contrast, some cyber-enabled crime is appropriately addressed by an anti-cybercrime instrument, for example, where the use of a computer increases:

(a) The scope of the offence, for example, by involving thousands of victims or the theft of millions of payment data records;

(b) The speed of the attack because a computer exponentially increases the ability to complete the offence;

(c) The scale of the damage or injury to victims; or

(d) The anonymity of the perpetrator.

[9] See article 18, paragraph 9, of the United Nations Convention against Transnational Organized Crime and article 46, paragraph 9, of the United Nations Convention against Corruption. Although the provisions in the two conventions differ somewhat, both offer substantial discretion to the requested States parties in providing assistance, particularly for coercive measures.

In applying these concepts, some cases of traditional crime, such as fraud and child exploitation, might also be reasonably viewed as within the scope of this negotiation. However, Member States should be judicious in the breadth of the cyber-enabled crime we seek to address so as not to distort long-standing criminal justice concepts. Long-standing criminal statutes and instruments do not lose their applicability simply because an offence involves some "cyber" component.

A global anti-cybercrime instrument should also call upon parties to enact legislation that criminalizes core cybercrime offences in a technologically neutral manner, while ensuring procedural safeguards. Criminalizing offences in a technologically neutral manner (i.e. criminalizing the activity affecting the confidentiality, integrity and availability of computer data instead of criminalizing the particular form or method used, such as phishing or ransomware) ensures that the substantive criminal provisions address not only present-day technologies and criminal techniques, but future technologies and techniques as well. As an illustration of just how quickly technology develops, even the draft Comprehensive Study on Cybercrime of 2013, with its explicit intent to be comprehensive, lacked details about technologies or techniques that were not widely used, or that were just emerging, at the time of the study, including ransomware, the Internet of things, cryptocurrency, and the rapid development and predominance of mobile technology. Reflecting this concern, one of the conclusions and recommendations agreed on by Member States in the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime was that Member States should ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used.[10] This is particularly important as we attempt to draft an enduring instrument that can adequately address the technologies of tomorrow and meet the needs of law enforcement practitioners both now and in the future.

Bearing these principles in mind, a global anti-cybercrime instrument should include the criminalization of the following:

(a) Illegal access, that is, accessing a computer or computer system without authorization;

(b) Illegal interception, that is, the real-time unlawful interception of the content of communications or traffic data related to communications;

(c) Data or system interference, that is, malware, denial-of-service attacks, ransomware, and data deletion or modification;

(d) The misuse of devices, that is, trafficking in or using credit card data, passwords and personal information that permit access to resources;

(e) Offences related to child sexual abuse materials;

(f) Offences related to computer-facilitated fraud, that is, manipulation of computer systems or data for fraudulent purposes such as phishing, the compromising of business emails and auction fraud;

(g) Offences related to infringement of copyright and related rights; and

(h) Provisions addressing attempt, aiding and abetting and conspiracy.

Furthermore, the laundering of the proceeds of cybercrime should also be criminalized. Finally, legal persons should be subject to criminal or civil and administrative sanctions if engaged in the cybercrimes that the instrument proscribes.

[10] See the report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021 (UNODC/CCPCJ/EG.4/2021/2).

Procedural authority for the collection and sharing of electronic evidence

In addition to the criminalization of substantive offences, a global anti-cybercrime instrument should also address the need for domestic legal authorities to preserve, collect and share electronic evidence, consistent with due process and the protection of human rights and fundamental freedoms. Some Member States have noted that, under their domestic law, traditional sources of procedural authority may not be applicable to intangible data or may not authorize the sufficiently rapid collection of volatile electronic evidence. As ever, outdated laws will not be sufficient to meet the many challenges of electronic crime investigations, including dealing with novel technologies such as widespread encryption and cloud computing services. Specialized sources of procedural authority to collect electronic evidence are therefore essential. These laws should be drafted with applicable technical concepts, as well as the practical needs of criminal investigators, in mind. More specifically, these sources of procedural authority should allow for:

(a) Expedited preservation of stored computer data;

(b) Production orders for computer data;

(c) Search and seizure of stored computer data;

(d) Real-time collection of computer traffic data; and

(e) Real-time collection of content data in cases of serious crime.

In addition, the new instrument should allow for cooperation to collect and obtain electronic evidence for any type of crime, not only cybercrime. Nearly all significant criminal offences involve electronic evidence, whether in the form of mobile telephone data, email, transactional data or other data, that is relevant to investigating and prosecuting crime. As a domestic matter, Member States need a modern legal evidence framework that permits the admission of electronic evidence in criminal investigations and prosecutions, including the sharing of electronic evidence with law enforcement partners internationally.

International cooperation

Beyond domestic laws, effective international cooperation on cybercrime relies on both formal, treaty-based cooperation, such as mutual legal assistance, and other means, such as traditional, authorized police-to-police cooperation. The new anti-cybercrime instrument should draw on effective tools for increasing international cooperation from existing treaties and ensure that it does not undermine existing instruments and ongoing international cooperation in the global fight against cybercrime. The provisions of the anti-cybercrime instrument related to international cooperation, including on mutual legal assistance, extradition, transfer of prosecution, confiscation of proceeds, including virtual currencies and the return of confiscated assets to victims, dual criminality and law enforcement cooperation, should adhere closely to the provisions of the Organized Crime Convention and the Convention against Corruption, including the appropriate safeguards and protections therein, which have been successfully implemented by the overwhelming majority of the Member States. In addition, the provision on mutual legal assistance should provide for broad assistance in obtaining electronic evidence pertaining to a criminal offence, whether or not the criminal offence was committed with the involvement of a computer system.

Technical assistance and capacity-building

UNODC studies note that more than 75 per cent of countries have a dedicated unit for cybercrime-related issues within existing law enforcement organizations, and about 15 per cent have a specialized, dedicated agency for cybercrime. This underscores the specialized nature of cybercrime investigations, including the need for specialized training. Moreover, the complexity of cybercrime offences and electronic or digital elements of traditional offences has increased significantly, which

creates additional demand for the training and maintenance of highly skilled investigators and technical experts.

Insufficient domestic capability is the most common reason why countries may not be able to cooperate effectively internationally. For most countries, international cooperation does not fail because of a lack of will, but because of limitations either in domestic law or in the expertise of law enforcement agencies. Many Member States are not well resourced with respect to the capacity of law enforcement authorities to combat cybercrime or handle electronic evidence. For example, in light of existing national priorities, some Member States face challenges in developing and retaining trained investigators, and forensic examiners, as well as in dealing with shortages in computer equipment and software. Accordingly, there is a broad international consensus that technical assistance and capacity-building for law enforcement institutions, including investigators, prosecutors and judges, remain the most urgent requirements for an effective international response to cybercrime. Moreover, as electronic evidence becomes a component of almost every type of crime, even non-specialized law enforcement officers will require some basic understanding of computer-related investigations.

The provisions of a cybercrime instrument related to technical assistance and capacity should include:

(a) Measures by Member States to initiate, develop or improve training programmes for their personnel responsible for preventing and countering cybercrime;

(b) Consideration by Member States, according to capacity, of affording one another the widest measure of technical assistance, especially for the benefit of developing countries and those countries that may disproportionately face cybercrime threats, in their respective plans and programmes to counter cybercrime;

(c) The establishment of mechanisms through which voluntary financial contributions from Member States could support the implementation of a cybercrime instrument;

(d) Consideration by Member States of making voluntary contributions to the UNODC Global Programme on Cybercrime and its related criminal justice capacity-building efforts.

Participation of society, entities and organizations

Countering cybercrime cannot be a siloed effort, given the complexity and multifaceted nature of the issue. An anti-cybercrime instrument should take into account the importance of active participation by individuals and groups, with due regard to gender parity, such as non-governmental organizations, civil society organizations, academic institutions and the private sector, in the prevention of cybercrime. Such participation can raise public awareness about the threats of cybercrime, ensure that the work of Member States is undertaken in a transparent manner and address substantive matters related to privacy, civil liberties and human rights. Furthermore, an effective instrument depends on the contributions of individuals and entities with expertise in the field of cybercrime. To implement a practical and effective anti-cybercrime instrument, the robust participation of experts in the field is essential.

Mechanisms for implementation

Determining whether a separate process is needed to review the future implementation of the instrument, and if so, what form it should take is too premature at this stage. There are various successful models to consider. Given the shortfall of resources available for technical assistance, consideration should be given to methods that rely on budget-friendly options to maximize donor contributions towards technical assistance. One such method would be to authorize the Commission on Crime Prevention and Criminal Justice, established pursuant to Economic and Social

Council resolution 1992/1, to consider all matters pertaining to the aims of the -cybercrime instrument. There is a successful precedent for such oversight vis-à-vis the Commission on Narcotic Drugs, which oversees the three international drug control treaties. As outlined in the above section on participation of society, entities and organizations, it is essential that the robust participation of public society, entities and organizations be considered when implementing any workstream emanating from an instrument. However, discussion on the mechanisms for implementation should be reserved until the scope of the instrument is further defined.