United States of America

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 UN General Assembly resolutions 74/247 and 75/282. The United States looks forward to working together with other UN 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 toward 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 creates 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 toward a global anti-cybercrime instrument. Unfortunately, while most of the world has worked to combat the COVID-19 pandemic, cyber criminals have exploited the resulting global shift and reliance on digital technologies. Cybercrime is a direct threat to the safety and well-being to societies and people around the world. There has been longstanding 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 UN 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 UN 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 to 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 UN and other intergovernmental and multi-stakeholder fora. 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 toward a useful instrument.

In particular, Member States should not delve into wide-ranging cyber-governance 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 government

responsibility, whereas cybersecurity is the responsibility of a range of public and private actors. The mandate of the AHC is focused on developing a criminal justice instrument on criminal matters to facilitate an international response to cybercrime, which involves defining and sanctioning criminal conduct in cyberspace. The AHC is not empowered to dictate global norms for non-criminal behavior online. Including cyber-governance 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 toward 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[1]. We can best build consensus for this new instrument and avoid political and divisive issues by drawing from existing instruments that have proven successful. We should be guided by the achievements implementing other UN criminal justice treaties, such as the UNTOC. The UNTOC has proven 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 UNTOC 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

[1] Resolution 75/282, Countering the use of information and communications technologies for criminal purposes. Adopted by the General Assembly on 26 May 2021 and available at https://undocs.org/en/A/RES/75/282.

good faith toward 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 Offenses

First and foremost, any new instrument should ensure domestic authority to collect and obtain electronic evidence for any type of crime. These authorities are 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 sharing electronic evidence of any type of crime, subject to a flexible dual criminality provision as contained in UNTOC and UNCAC.[2]

In addition, effective international cooperation requires Member States to have adequate domestic legislation that criminalizes core cybercrime offenses. A shared understanding of core substantive offenses and supporting procedural authorities among Member States is essential to avoid creating safe havens for cybercriminals. UNODC studies 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 procedural authorities to support effective cybercrime investigations is settled. As a result, practitioners have two decades of accumulated and varied experience investigating cybercrime that demonstrates the continuing viability of commonly adopted substantive and procedural authorities to investigate cybercrime.

[2] UNTOC Article 18, paragraph 9; UNCAC Article 46, paragraph 9. Although the provisions in the two conventions differ somewhat, both offer substantial discretion to the receiving states parties in providing assistance, particularly for coercive measures.

A new anti-cybercrime instrument should define and apply to cyber-dependent crimes, which are crimes in which a computer or data is the target of the criminal activity, as well as certain cyber-enabled crimes, i.e. crimes in which a computer was used to facilitate the crime. This first and principal category of offenses to be defined by this new instrument are those that cannot be committed without the misuse of computers or network systems and 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 crime offenses, 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, like 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 through computers.

In contrast, we should be careful not to treat traditional crimes as a "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 a computer system in that conduct. In contrast, some cyber-enabled crime is appropriately addressed by an anti-cybercrime instrument where, for example, the use of a computer increases

- the scope of the offense, for example thousands of victims or the theft of millions of payment data;
- the speed of the attack because a computer exponentially increases the ability to complete the offense;
- the scale of the damage or injury to victims; or

- the anonymity of the perpetrator.

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 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 offense involves some "cyber" component.

A global anti-cybercrime instrument also should call upon parties to enact legislation that criminalizes core cybercrime offenses in a technology-neutral manner, while ensuring procedural safeguards. Criminalizing offenses in a technology-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, like 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 from 2013, with its explicit intent to be *comprehensive*, lacked details about technologies or techniques that were not widely used, or 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 UN Expert Group 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."[3] 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

- illegal access, i.e. accessing a computer or computer system without authorization;
- illegal interception, i.e. real-time unlawful interception of the content of communications or traffic data related to communications;
- data or system interference, i.e. malware, denial of service attacks, ransomware, data deletion or modification;
- misuse of devices, i.e. trafficking or using credit card data, passwords and personal information which permit access to resources;
- offenses related to child sexual abuse materials;
- offenses related to computer-facilitated fraud, i.e. manipulation of computer systems or data for fraudulent purposes such as phishing, business email compromises, and auction fraud;
- offenses related to infringements of copyright and related rights; and
- provisions addressing attempt, aiding and abetting and conspiracy.

[3] UNODC/CCPCJ/EG.4/2021/2, Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021, available at https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf.

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 the instrument proscribes.

Procedural Authorities for Collection & Sharing of Electronic Evidence

In addition to the criminalization of substantive offenses, 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 procedural authorities may not be applicable to intangible data or may not authorize 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 procedural authorities to collect electronic evidence are therefore essential. These laws should be drafted with applicable technical concepts in mind as well as the practical needs of criminal investigators. More specifically, these procedural authorities should allow for

- expedited preservation of stored computer data;
- production orders for computer data;
- search and seizure of stored computer data;
- real-time collection of computer traffic data; and
- real-time collection of content data in cases of serious crime.

In addition, the new instrument should allow cooperation to collect and obtain electronic evidence for any type of crime, not only cybercrime. Nearly all significant criminal offenses

involve electronic evidence, whether in the form of mobile phone data, email, transactional data, or other data, which 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 sharing 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 mutual legal assistance (MLA), 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 UNTOC and UNCAC, including the appropriate safeguards and protections therein, which have been successfully implemented by the overwhelming majority of UN Member States. In addition, the provision on MLA should provide for broad assistance in obtaining electronic evidence pertaining to a criminal offense, whether or not the criminal offense was committed with the involvement of a computer system.

Technical Assistance & Capacity Building

UNODC studies note that more than 75 percent of countries have a dedicated unit for cybercrime-related issues within existing law-enforcement organizations, and about 15 percent 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 offenses and electronic or digital elements of traditional offenses has increased significantly, which places additional demands for the training and maintenance of highly skilled investigators and technical experts.

Insufficient domestic capability is the most common reason that countries may not be able to cooperate effectively internationally. For most countries, international cooperation does not fail from lack of will, but from limitations either in domestic law or in the expertise of law enforcement agencies. Many Member States are not well-resourced with respect to law enforcement capacity for combating cybercrime or handling 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 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:

- Measures by Member States to initiate, develop, or improve training programs for their personnel responsible for preventing and countering cybercrime.
- Consideration by Member States, according to capacity, to afford 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 programs to counter cybercrime.
- Establishment of mechanisms through which voluntary financial contributions from Member States could support the implementation of a cybercrime instrument.
- Consideration by Member States to make voluntary contributions to the United Nations Office on Drugs and Crime Global Program on Cybercrime and its related criminal justice capacity building efforts.

Participation of Public 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 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 future implementation of the instrument, and if so, what form it should take is too preliminary 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 to technical assistance. One such method would be to authorize the Commission on Crime Prevention and Criminal Justice, established by the Economic and Social Council Resolution 1992/1, to consider all matters pertaining to the aims of the anti-cybercrime instrument. There is 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 *Participation of Society, Entities, and Organizations* section, it is essential that the robust participation of public society, entities, and organizations be considered when implementing any workstream from an instrument. However, discussion on mechanisms for implementation should be reserved until the scope of the instrument is further defined.