**Comments of the United States of America to the**
**Draft Comprehensive Study on Cybercrime**
**August 22, 2016**

The Permanent Mission of the United States of America presents its compliments to the Secretariat of the United Nations Office on Drugs and Crime (UNODC), and has the honor to respond to the invitation contained in Note Verbale CU2016/50/DTA/OCB/CSS to provide comments on the Draft Comprehensive Study on Cybercrime (Draft Study) prepared under the auspices of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (Expert Group). The United States appreciates the diligent work of the Secretariat in translating the Draft Study to permit the broadest participation by countries.

*Summary*

The United States believes the Draft Study has both positive elements and less useful inclusions. The Draft Study lays out important challenges in addressing cybercrime, and from the data collected, it is clear that the international community is actively taking steps to overcome these challenges through specific actions. These include: a) capacity building and technical assistance, b) participation in existing multilateral instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe's Budapest Convention on Cybercrime (Budapest Convention), c) participation in a 24/7 network for rapid assistance in electronic evidence matters, d) strengthening public-private partnerships with Internet service providers, and e) development of effective national legal frameworks that criminalize specific behaviour and promote efficient international cooperation. These actions are examined in further detail below.

While we concur with many of the concerns identified in the Draft Study, some of the challenges and proposed responses detailed by its authors either are not substantiated by the data in the Study itself, or reflect a potential lack of understanding of cybercrime and the basic practice and purpose of international cooperation. In this context, it is important to highlight that the Expert Group never requested that the Secretariat formulate any such recommendations to Member States as part of the Study; while they are presented as "options," these ideas are clearly policy recommendations which should be reserved to Member States.[1] Of particular concern, many of the key findings and options summarized on pages xi-xiv of the Draft Study, which also appear at the end of each chapter, appear to respond to a select group of political viewpoints presented in previous sessions of the Expert Group. As such, the United States believes that all of the findings and options presented in the Draft Study are not the product of deliberation and consensus by the Expert Group. Therefore, all key findings and options should be removed from where they appear in the Draft Study.[2] We call on the Secretariat to delete these findings and

[1] As the March 5, 2013, report of the Secretary-General (E/CN.15/2013/24) at P18 notes, "[t]he findings and options contained in the study and the executive summary were prepared by UNODC on the basis of empirical information provided and are not intended to constitute recommendations."

[2] Importantly, the report of the Secretary General at P17 notes that "[i]n discussions concerning the cybercrime study, it was noted that there was broad support for capacity-building and technical assistance, and for the role of the UNODC in that regard. Diverse views were expressed regarding the content, findings and options presented in the study.

options from the Draft Study as they otherwise may distort the interpretation of valuable information collected through this process.

As one example of this unhelpful distortion, the Draft Study proposes (despite no mandate from the Expert Group to propose any such action) the promulgation of a new international instrument on cybercrime, the supposed purpose of which is to address perceived gaps and weaknesses in existing instruments and to strengthen international cooperation. This proposal rests on the incorrect perception of the existence of "clusters" of specific countries that are party to the same legal instrument and have the necessary powers and procedures to cooperate among themselves, but are restricted to traditional modes of cooperation with countries which are not in a similar or the same "cluster." The Draft Study also purports to identify a "lack of a common approach" at a global level which negatively affects the ability of governments to request or provide legal assistance, including the expedited preservation of data and evidence; increases response times for requests; and limits agreement on permissible direct access to extraterritorial data. Finally, the Draft Study concludes that multiple law enforcement information-sharing networks and a degree of variance in procedural cooperation safeguards are challenges that must be overcome via a new global legal instrument on cybercrime.

However, the Draft Study fails to articulate any challenge that cannot be more effectively overcome through robust capacity-building, effective domestic laws and procedures to support international cooperation, and participation in an existing legal instrument. The Draft Study also fails to highlight that efforts to develop a new global instrument (which would likely take years, if not decades) would likely undermine both political will and distract financial resources from capacity building to address cybercrime as an urgent problem that faces many law enforcement and criminal justice institutions today.

At the same time, the Draft Study does highlight the role of technical assistance, accession to existing instruments, and participation in a 24/7 network as steps that have contributed effectively to positive global awareness and national capacity to respond to cybercrime. Countries which receive training and capacity-building, join an existing multilateral treaty, and/or engage in active international cooperation using existing frameworks have dramatically increased their ability to combat cybercrime, thus obviating any possible need for a new instrument. In a world of limited resources, the Draft Study – despite the language contained in its key findings and options section – supports the conclusion that both time and money are better spent on training and capacity-building, rather than uncertain and lengthy negotiation of a new instrument on cybercrime. The United States examines some of these more realistic and effective opportunities below in further detail.

*Evolutions in Cybercrime Since 2013*

The United States believes that the Draft Study provides a useful "snapshot" of global trends in cybercrime as of 2013. The Draft Study also usefully identifies global best practices in cybercrime prevention, investigation and prosecution and underlines the importance of capacity building. Furthermore, the Draft Study also makes it clear that public-private partnerships are essential to cybercrime standards, and central to cybercrime prevention. Internet service providers play an important role in cybercrime prevention, as well as criminal investigation.

Some providers go further and take proactive steps to protect their customers. Every Internet communication must traverse one or more service providers, whether a private company, government, or academic institution. Providers will retain subscriber information, communication logs, and content, all of which may be critical evidence for a criminal investigation. The concept of public-private sector cooperation is one that merits further exploration by Member States.

However, no study in time can anticipate future developments. Change is the only constant in cybercrime as cybercriminals exploit new communications methods and technological changes on the Internet. Contrary to some views expressed in prior Expert Group meetings, even as the threat evolves, the fight against cybercrime has not stood still but continues to improve. The fight against cybercrime is a top priority among governments in virtually every multilateral body. Businesses are strengthening alliances to share information on ways to better defend against cyber threats. Rising levels of public awareness place greater pressure on governments to reform their policies and practices. Unfortunately, the Draft Study does not cover important recent developments in the international community's response to cybercrime, such as the work of the UNODC's Global Program on Cybercrime, which offers urgent capacity building training and technical assistance to Africa, Asian, and Eurasian countries. Financially supported by donor countries, including by the United States, the Global Program has demonstrated its value in strengthening law enforcement, including prosecutors, and judicial capacity in concrete ways, and has resulted in concrete and successful investigations and prosecutions.

Similarly, the Draft Study does not capture the hard work of numerous countries to enact national cybercrime legislation since 2013, and the continued growth in accession to the Budapest Convention with 15 additional ratifications since the Draft Study was undertaken.[3] Indeed, countries with diverse legal systems from all regions around the globe have acceded to the Budapest Convention, demonstrating the Convention's continued viability as the premier international instrument to address cybercrime. While it includes a number of references to the UNTOC, the Draft Study also fails to accurately and fully reflect the value of the UNTOC, which over the last 13 years has proven to be an effective tool to facilitate international cooperation against various forms of transnational organized crime, including cybercrime.

*Technical Assistance and Capacity-Building*

The Draft Study makes clear that there is effectively a global consensus on online conduct which should be criminalized in national legislation, as well as the necessary investigative and procedural authorities to permit the investigation and successful adjudication of cybercrime. The data collected by the Draft Study also underscores the dire need for capacity building and technical assistance, in particular for developing countries in Africa, the Americas, and Asia. This convergence of agreement on key priorities for reform and a sense of urgency among beneficiary countries to receive technical assistance are important to note as we consider potential options to address cybercrime. In fact, many countries in these regions have for years

[3] Since 2013, five countries (Canada, Israel, Turkey, Poland and Luxembourg) completed their ratifications and the Convention entered into force in three others (Panama, Mauritius and Sri Lanka). Twelve countries are in the accession process.

received training and other assistance from United States law enforcement agencies, and increasingly benefit from assistance from international organizations like UNODC. These steps strengthen the ability of States to investigate domestic offenses and as a result, to cooperate effectively with international partners.

Capacity building and technical assistance directed to practitioners will strengthen national responses to cybercrime by improving national legislation and law enforcement technical and forensic skills. Improved capacity has the cross-cutting benefit of affording countries the practical ability to meet their international obligations under existing instruments for all types of crime. As the Study notes, the data collected in this Study have "unique relevance" for all crimes because it is "hard to imagine a 'computer crime', and perhaps any crime, that will not involve electronic evidence linked with internet connectivity." Therefore, even in the absence of consensus on some proposals to address cybercrime, there is a clear and universal benefit to investing in technical assistance that is both tailored to cybercrime-specific challenges and also broader in nature. The combination of global political agreement on (a) priority areas of reform needed to address cybercrime, (b) desire for capacity-building assistance, and (c) clear practical benefits for law enforcement and criminal justice officials simply does not exist for many other proposals to combat cybercrime – including the Draft Study's recommendation to develop a new global instrument. By contrast, it seems readily apparent that sufficient investment in domestic reform, supported by robust technical assistance programs, on the basis of existing multilateral treaties, would make a significant difference in resolving many of the concerns and purported challenges identified in the Draft Study.

*Regional instruments on cybercrime are effective for their members*

In 2013, less than half of responding countries believed that their substantive and procedural national laws were sufficient to address cybercrime. Of these countries, only half planned to address the shortcomings in national law.[4] This suggests that many countries still do not appropriately prioritize cybercrime or may need assistance in raising the awareness of decision makers to cybercrime risks to economic development and national security. The Draft Study asserts that the diversity of national cybercrime laws, possibly correlated with the existence and application of multiple instruments, may lead to cooperation between countries at the regional or "cluster" level, and that these clusters are not "well-suited" to the global nature of cybercrime.

According to the Study, there are 19 multilateral instruments relevant to cybercrime which show a base level of common core provisions of 14 categories of cybercrime.[5] In addition, a "significant amount of cross-fertilization" exists among all instruments, which reflects for most regional instruments a common source in the Budapest Convention.[6] Furthermore, no region of the globe is excluded from the reach of at least one regional instrument, and the Budapest Convention is open to accession by any country. Accordingly,

[4] Draft Study (2013), p. xviii.

[5] The Draft Study notes that there are "significant divergence in substantive areas addressed." National law will always respond to local circumstances, so it is not unusual to have differences. However, these differences do not present practical challenges in cooperation.

[6] Draft Study (2013), p. xix.

countries have numerous examples of substantive law in both multilateral instruments and the national laws of their regional partners which illustrate the types of behaviour that should be criminalized in national legislation on cybercrime. Importantly, the Draft Study notes that membership in a multilateral cybercrime instrument results in increased sufficiency of national criminal law, and that current multilateral provisions are considered effective by the countries that have joined an existing instrument. Moreover, the Draft Study has not identified any significant gap in national legislation which cannot be filled by acceding to a regional instrument or modelling national law on existing instruments. Thus, we find that a new global instrument would provide little or no added value that cannot be obtained immediately through training and capacity-building and domestic reform efforts.

Contrary to the finding that cooperation "clusters" may form because different States may become party to separate and distinct legal instruments, rather than one single global instrument, the Draft Study does not identify any difficulty in enforcement or international cooperation experienced by countries that are members of different multilateral instruments, i.e., different "clusters." In fact, membership in a multilateral instrument is not a requirement for international cooperation on any form of crime, and in practice has posed no difficulty to cooperation among States who are members of different "clusters." For example, the United States has cooperated successfully with a wide range of States that are not members of the Budapest Convention, which came into force for the United States in 2006. Given the Draft Study's conclusion that membership in any multilateral cybercrime instrument results in increased sufficiency of national criminal law, it appears that one practical solution for a country seeking either a model for national legislation or to improve international cooperation is simply to accede to an existing multilateral instrument. It is self-defeating for countries to delay joining an existing instrument, since there is no assurance that consensus on a more effective new instrument will be achieved.

*International consensus on "core" cybercrime offenses*

There is broad agreement among responding States on the specific, core offenses that are directly related to cybercrime, although countries have different approaches to other, tangential but substantive offenses, such as computer misuse tools, racist and xenophobic expression, and solicitation of children. Importantly, these divergences derive from underlying legal and constitutional differences, including differing conceptions of rights and privacy[7], and not from differing conceptions of typical, substantive cybercrimes. For example, some responding countries reported limitations to free expression. Other "socio-cultural" elements of some limitations are reflected in national law, and in regional instruments to which the country may be a party.[8] However, these differences generally do not prevent cooperation internationally. The United States engages in international cooperation on cybercrime with countries that have diverging conceptions of rights and privacy, including countries that are not party to the same multilateral instruments as the United States.

Similarly, disparities in punishment where some types of online criminal conduct may not be treated as seriously as crimes in the "physical world" do not restrict the scope of or possibility for States to engage in international cooperation. In this context, the United States

[7] Draft Study (2013), p. xix.
[8] Draft Study (2013), p. xxi.

notes that the plethora of existing international instruments on cybercrime already provide extensive and substantive guidance to their States parties on criminalization and enforcement measures, and it seems unlikely that those States who have already ratified or acceded to one of the 19 existing cybercrime instruments would see value in, or would actively work to negotiate, a new global instrument that provides a significantly different legal standard. It further seems unlikely that a new global instrument could provide new value for international cooperation that is not already possible to achieve through existing bilateral and multilateral practices and agreements.

*Relevance and Importance of Harmonizing Legal Frameworks*

While one-third to one-half of countries outside of Europe reported in 2013 that their national legal frameworks are insufficient, approximately one-third of responding countries reported a high degree of harmonization with prevailing international standards on cybercrime, while the remainder viewed their legislation as "partially" harmonized with international standards. The Draft Study judged that harmonization of cybercrime laws to be fairly high in 2013, and that harmonization has very likely increased as more countries enacted cybercrime legislation. This is unsurprising because the majority of regional instruments are derived from the Budapest Convention, the prevailing international standard. In this context, it appears that the existing landscape of multilateral instruments on cybercrime already contributes positively to greater harmonization of national legislation.

The Draft Study asserts incorrectly that the data collected reveals that international cooperation against cybercrime is hampered by (a) the diverse range of regional cybercrime instruments and national cybercrime laws and (b) the purportedly insufficient harmonization of core cybercrime offenses and police investigative authorities. Some of these findings are simply not supported by the disclosed data[9], and some are directly contradicted by the report's own analysis.

In this context, the Draft Study's emphasis on "harmonization," which appears to mean replicating the exact law in every country, is fundamentally misplaced. International cooperation on criminal matters does not depend on a precise match among the diverse criminal laws among countries. In fact, international cooperation against many forms of crime would be impossible if this were the actual standard. Instead, cooperation is premised on the adoption of criminal laws which, though tailored to fit within national legal frameworks, nonetheless sanction the same or similar underlying illicit activity. Satisfying this dual criminality requirement becomes insurmountable if countries must name offenses identically and include identical elements. As a result, treaties omit exact harmonization requirements, and instead focus on acts. The Draft Study itself notes that "[a] key factor in establishing dual criminality is the substantive underlying conduct, and not the technical terms or definitions of the crime in national laws."[10] This approach leaves countries free to implement their obligations -- if they do at all -- in differing ways consistent with their legal systems.

[9] There is no indication in the Draft Study of the responses of specific countries to specific questions. The questionnaire's raw data could assist the Expert Group in assessing global strengths and weaknesses in the fight against cybercrime.

[10] Draft Study (2013), p. 202.

Importantly, despite its own recommendation to create a new global instrument, the Draft Study recognizes that national law, and not international treaties, is the basis for harmonization of criminal law as well as authorization for international cooperation.[11] Countries that lack domestic legislation on cybercrime, or do not permit their national authorities to share information, are unable to cooperate internationally on cybercrime. Few countries act contrary to their national interests by discouraging international cooperation. The Draft Study thus reaffirms the bedrock requirement that each member state should pass domestic legislation on cybercrime. Similarly, countries should pass national procedural laws to authorize domestic law enforcement to investigate cybercrime and cooperate internationally by sharing electronic evidence through formal means such as MLA or operationally though police-to-police cooperation. The solution to improving international cooperation is thus not one of exact harmonization of cybercrime laws, but rather to pass national laws which authorize international cooperation; there is no clear need for additional normative deliberations at a global level to achieve greater law enforcement and legal cooperation on cybercrime.

Countries vary more broadly with respect to investigative measures authorized by domestic law. While there is no practical difference between "cyber-specific" and general investigative powers, the Draft Study notes that countries with specific cybercrime legislation will also have sufficient laws authorizing investigative powers such as production orders to providers, search and seizure of data, and preservation schema.[12]

Finally, the Draft Study's conclusion that there is no global mechanism to harmonize the rules for the admissibility of electronic evidence also misunderstands the nature of evidence rules. Traditional "chain of custody" issues which address the authenticity of evidence introduced at trial is just one concern. The more serious concern is not merely about the authenticity and admissibility of electronic evidence at trial, which are legal questions determined by national law. Rather, the practical problem is obtaining in the first place such evidence in a forensically sound and reliable manner because some countries do not have the law enforcement capacity and expertise to obtain electronic evidence in their jurisdiction, and the operational ability to share that evidence. Once again, the challenge clearly presented by the data collected in the Draft Study is not a question of harmonization, but rather of capacity, training, and technical assistance.

*International Cooperation*

Treaty-based forms of international cooperation such as mutual legal assistance requests and traditional police-to-police cooperation predominate in cybercrime investigations. According to the Draft Study, over 70% of countries use mutual legal assistance requests with bilateral treaties invoked in 60% of cases, and multilateral instruments invoked in 20% of cases. Globally, over 60% of countries are not parties to any multilateral cybercrime instrument, with the result that they have no international legal obligation to include specialized cybercrime investigative powers in national legislation, or to carry out requests for cooperation from foreign partners. However, the Draft Study also acknowledges that the "absence of national legislation

[11] Draft Study (2013), p. 55.
[12] Draft Study (2013), p. 125.

on extradition or mutual legal assistance does not prevent countries from engaging in international cooperation in cybercrime matters."[13] This is likely due to the willingness of a country to extend cooperation on a police-to-police basis, without reference to treaties. Thus, countries should join one or more existing multilateral instruments for an immediate improvement in their ability to cooperate internationally on cybercrime.

Despite this clear and widely acknowledged ability for States to engage in cooperation on any form of crime using existing bilateral and multilateral instruments, as well as police-to-police cooperation, the Draft Study asserts that an analysis of existing formal and operational mechanisms is:

> "unable to find that the current global cooperation situation is sufficient. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments; a lack of response time obligation; multiple informal law enforcement networks, and variance in cooperation safeguards represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters."[14]

This analysis ignores the Draft Study's own conclusions that (a) the divergences among multilateral instruments in cooperation provisions do not reflect a fundamental difference in an approach to cybercrime, but instead reflect constitutional and cultural differences, and (b) lack of membership in a multilateral instrument does not prevent international cooperation. As noted above and in the Draft Study, there is already a high degree of harmonization among the national law of most countries that have cybercrime laws. Second, regional instruments and the Budapest Convention all promote expedited cooperation and information sharing, even if they differ slightly in terms of the particular obligations placed upon States who are party to different instruments. Third, the existence of multiple operational law enforcement networks is hardly a weakness, but rather a strength; many law enforcement authorities regularly participate in multiple and overlapping networks to address a wide range of crimes, providing them with a variety of channels to request and obtain police-to-police cooperation. Finally, when countries adhere to their human rights responsibilities, variation in cooperation safeguards also does not prevent effective international cooperation.

Thus, the United States cannot find logic or substance in the assertion of the Draft Study quoted above; if a State wishes to engage in international cooperation on cybercrime and has taken the domestic steps necessary to facilitate that process, a State can and will effectively cooperate with other jurisdictions on cybercrime. In this context, greater legislative assistance and capacity-building will improve the ability of criminal justice authorities to engage in international cooperation and combat cybercrime. The Draft Study presents no persuasive reasons that a new global instrument is necessary or appropriate in this regard.

*Cybercrime is transnational organized crime*

Furthermore, this Draft Study's analysis does not fully recognize the contribution of the UNTOC in the context of international cooperation on cybercrime, which is surprising given

[13] Draft Study (2013), p. 200.
[14] Draft Study (2013), p. 208.

UNODC's role as guardian of this Convention and the nearly universal status of its ratification. Although the Draft Study asserts that over 60% of countries are not party to any multilateral cybercrime instrument, these countries are likely parties to the UNTOC, even if not yet implemented. In fact, the United States has relied on the UNTOC as a legal basis for cooperation in numerous cases related to both cybercrime and electronic evidence. We thus believe it is possible for States Parties to the UNTOC to do so more regularly and with more intention.

To help increase awareness of this possibility, it may be helpful to reinforce that, as the Draft Study notes, approximately 80% of cybercrime originates in some form of organized crime, usually underground markets, with responsibilities shared by criminal participants.[15] The UNODC Digest of Organized Crime Cases notes that the presence of an organized criminal group as a factor in all cybercrime cases substantially diminishes the role of isolated hackers as the main actors in cybercrime. Indeed, the image of a "lone hacker" as the perpetrator of cybercrime is no longer accurate in most cases; instead, organized, transnational groups often perpetrate the largest data breaches and attacks on critical infrastructure. The most significant data breaches, "carder forums" where identity information, credit and bank card information are sold, require a high degree of organization to implement, usually in criminal groups or loose networks with a clear hierarchy.[16] Such perpetrators would clearly meet the definition of an organized criminal group pursuant to the UNTOC.

The Draft Study notes that one country in western Africa cited the "development of cybercrime groups that are more and more organized and possessing a transnational dimension."[17] This finding comports with the experience of the United States. The Draft Study also notes that cybercrime has transformed from a low volume crime to a common high volume crime that is "organized and industrial-like."[18] As noted in the Draft Study, the great majority of cybercrime is committed by organized groups, and the UNTOC can facilitate information and evidence sharing for cybercrime investigation in these cases. Based on requests that the United States has received to date, an increasing number of countries recognize the applicability of the UNTOC to cybercrime, or criminal matters involving electronic evidence. To this end, it seems clear that States which are interested in combating cybercrime should consider ways to join or apply existing instruments like the UNTOC, and to ensure that national authorities are aware of their ability to engage in international cooperation and to investigate and prosecute cybercrime using the UNTOC.

*Capacity Building for Law Enforcement*

Because electronic evidence is often relevant to many types of crimes, strengthening law enforcement capacity on anti-cybercrime efforts will also improve capacity to investigate other types of crimes. In particular, computing device[19] forensic capacity will improve investigations

[15] Draft Study (2013), p. xvii.
[16] Draft Study (2013), p. 45.
[17] Draft Study (2013), p. 45.
[18] Id.
[19] A "computing device" may be any device capable of processing data, such as the "traditional" computer, a smartphone, and tablet.

into many crimes. Cybercrime victimization rates are higher in developing countries, which underlines the need to strengthen the national capacity of these countries to tackle the problem.[20]

As of 2013, over 90% of responding countries had in place some capability for investigating cybercrime and handling electronic evidence.[21] However, all responding African countries and over 80% of countries in the Americas, Asia, and Oceania underlined a need for capacity building and technical assistance.[22] The most common need is training in general cybercrime investigative techniques, in addition to forensic capability, prosecutorial training, and judicial training.

In many cases, the problem appears to be an absence of knowledge and technical skill, not an absence of law. The Draft Study notes that 70% of law enforcement with responsibility for cybercrime in developing countries lack computer skills and equipment, and do not receive regular training in online investigation and electronic evidence. Only half receive training more than once a year. The urgent need for capacity building is palpable with *all* responding countries in Africa and over 80% of countries in the Americas, Asia, and Oceania reporting that they needed increased technical assistance on cybercrime. The most commonly cited need for technical assistance is training for general cybercrime investigative techniques. About 60% of countries indicated that their law enforcement agencies need this training.

Notably, prosecutorial skills with respect to cybercrime are typically lower than investigators.[23] Almost 80 % of more highly developed countries reported some type of prosecutorial cybercrime specialization. This specialization may be in a specialized unit or agency, or even specialized personnel who are not organized as a separate unit.[24] In contrast, less than 60% of less developed countries report prosecutorial cybercrime specialization.[25] The less developed countries reported that even specialized prosecutors either had basic or no IT skills, and intermediate computer equipment or none at all. [26] Additional training and exchange of information is essential for prosecutors. Similarly, judicial training on cybercrime law, evidence collection, and basic computer knowledge is a priority among developing countries.

As such, the United States reiterates its view that the urgent delivery of technical assistance and capacity-building is the only action proposed in the Draft Study that responds directly to the concerns voiced by developing countries regarding the availability and compatibility of national legal frameworks to combat cybercrime. Technical assistance and capacity-building provide a meaningful and realistic chance of improving the global landscape of law enforcement to combat cybercrime in the near future, and is the only clear area of broad

[20] Draft Study (2013), p. xviii
[21] Draft Study (2013), p. xxiii.
[22] Id.
[23] Draft Study (2013), p. 174.
[24] Draft Study (2013), p. 173.
[25] Id.
[26] Draft Study (2013), p. 175.

agreement among countries that responded to the Draft Study questionnaire and/or participated in previous meetings of the Expert Group[27].

*Data preservation*

The Draft Study points out that the response times for formal mechanisms for cooperation remain on the order of months for both extradition and mutual legal assistance requests.[28] For a government like the United States that handles roughly 12,000 active incoming and outgoing requests for mutual legal assistance and extradition at any given time, these response times are not unusual or inappropriate, and the Draft Study mistakenly asserts that these response times present a challenge to "the collection of volatile electronic evidence."[29] There is a difference between the preservation and the collection of evidence, and the formal response time needed to produce the collected evidence. If data availability is assured, for example by a prompt and well-executed request for preservation followed close in time by a sufficient mutual legal assistance request, there is no reason that formal responses for assistance in cybercrime cases should be faster than in other types of criminal matters.

The Draft Study also notes specifically that fora for operational cooperation (described as "informal" cooperation) such as the 24/7 networks offer very fast response times for preservation of data. Despite the 24/7 networks' clear and obvious value for facilitating data preservation, the Study notes that in 2013 the 24/7 networks were used in only 3% of the total number of cybercrime cases handled by law enforcement[30], indicating that a large number of countries could drastically improve their ability to respond quickly to cybercrime by simply joining one or more 24/7 networks that permit rapid requests for assistance, including preservation of data. In some cases, the requested country may provide data through the network if permitted by that country's national law.

Despite ready solutions that are available to Member States such as increased use of 24/7 networks, greater capacity building and technical assistance, and the availability of 19 existing multilateral instruments, the Draft Study also asserts that a "lack of a common approach" means that requests for preservation may not be easily fulfilled because of "a lack of an international obligation to ensure such facility."[31] However, this suggestion misconceives the purpose of a 24/7 network, which is intended to be a channel for police-to-police cooperation that is more flexible than could be provided by the terms of any instrument. Indeed, the growth of the 24/7 network since 2013 demonstrates the value that countries place on these operational relationships, without the need for an instrument to mandate a specific channel for cooperation. In this context, the Draft Study fails to demonstrate in any meaningful way how a new legal instrument could achieve new standards in data preservation and data availability that cannot already be achieved through the simple participation of States in existing channels for cooperation.

---

[27] The Draft Study also notes that "a very small proportion," estimated at 3% of specialized prosecutors was reported to have been trained by international or regional organizations. The UNODC's Global Program intends to change that, and has provided additional training since 2013 to Central American, African, and Asian countries.

[28] Draft Study (2013), p. xxiv.

[29] Draft Study (2013), p. xxv.

[30] Id.

[31] Ibid.

Moreover, mandating a specific response time and capability in a 24/7 network risks leaving behind some countries, who are politically willing and prepared to cooperate internationally. The existing networks require only best efforts to assist, and the United States has cooperated successfully with countries which do not have similar expertise and capacity. Requiring countries to meet a degree of expertise or responsiveness which they may not yet have likely will lead to fewer countries participating in the network. On balance, it is preferable to have a country participate in the network, and through experience improve its capacity, than not to participate at all. For the Group of Seven (G-7) and Council of Europe 24/7 networks, regular training is also available to support and strengthen the network.

Once again, capacity-building and technical assistance will play a critical role in ensuring the timely preservation and provision of data and evidence. Even when a country has domestic legislation in line with prevailing international norms, cooperation mechanisms nevertheless depend on the existence of a competent and well-organized foreign counterpart. The law enforcement agencies of some countries are under-resourced and frequently suffer from a capacity shortage. This shortage affects cybercrime investigation and impacts international cooperation across all law enforcement issues in cybercrime: prevention, investigation, prosecution, and adjudication. Assistance to developing countries to strengthen capacity should thus be an international priority.

Furthermore, the Draft Study notes that existing "gaps" in procedural investigative powers, in particular a lack of any domestic scheme to preserve electronic data expeditiously, remains a challenge for a number of countries. These gaps can easily be resolved through national legislation. Moreover, jurisdictional issues generally do not prevent prosecution or cooperation. As the Draft Study itself notes, it is likely that at least one, if not more, countries can assert jurisdiction over online criminal conduct as well as jurisdiction over the defendant. Thus, it is not necessary or appropriate to consider a new instrument as proposed in the Draft Study, as the challenges detailed above can and should be addressed through robust legislative assistance, capacity-building, and active dialogue between law enforcement agencies through networks.

*There is no need for a new instrument on cybercrime*

As noted above, despite not having been requested by the Expert Group to develop such options and recommendations, the Draft Study proposes the promulgation of a new international instrument on cybercrime purportedly to address perceived gaps and weaknesses in existing instruments and to strengthen international cooperation. As previously detailed, this proposal rests on a misperception that countries cannot work together because: (a) "clusters" of specific countries are party to the same legal instrument, but are purportedly limited in their ability to cooperate with other countries outside their "cluster"; (b) variation in national legislation and obligations under existing multilateral instruments negatively affects requests for assistance, response times, and agreement on access to data; and (c) multiple information-sharing law enforcement networks and minimal variance in procedural cooperation safeguards limit cooperation. However, as demonstrated above, these justifications are clearly not supported by

the Draft Study itself, and can easily be overcome through tangible, accessible, and immediate solutions like domestic reform and technical assistance.

First, any country with sufficient legislation and investigative capacity will be able to preserve or obtain data requested by foreign partners, whether or not that country is a party to a multilateral instrument. In some cases, a country will have an immediate preservation scheme supported by a skilled 24/7 network point of contact who can receive and execute requests for assistance. In other instances, a request for preservation may require legal process in the requested country. Where a request for preservation requires legal process, the requesting country must provide sufficient information to satisfy the requested country's legal process to obtain the data. This is not a stringent burden, and in practice, there is little or no difference in efficacy to preserve the evidence. In either case, the objective of preserving the evidence is achieved.

Second, response times for preservation of data are usually very prompt, i.e. on the order of days, if not hours. Once the data is preserved, a sufficient MLA request will generally facilitate production of the data. In these instances, the challenge to effective cooperation is preparing a valid and sufficient request. On this point, the UNODC's Mutual Legal Assistance Writing Tool holds the promise of improving MLA requests, which will minimize delays in response. Over 70% of responding countries used mutual legal assistance requests in cybercrime cases.[32] Of this number, almost 60% used bilateral instruments and 20% used multilateral instruments.

Third, multiple law enforcement information-sharing networks improve both the likelihood that a requesting country will get a response, as well as the rapidity of a response. Each country should ensure that national law does not prohibit law enforcement information sharing with international partners, and that there is a domestic commitment to international cooperation.

Finally, there is no consensus on direct law enforcement access to extra-territorial data, whether through authorized "remote" searches or through technical means such as remote access tools. The Draft Study notes that over one-third of responding countries did not respond to the question in the Questionnaire concerning law enforcement authority for 'trans-border' access, which raises a serious question about the reliability of the data. This issue alone does not justify the promulgation of a new instrument, because even in the absence of trans-border authority, countries can continue to take advantage of robust police-to-police 24/7 cooperation networks.

In this context, the United States fails to see how – even if the authors of the Draft Study had an appropriate mandate from the Expert Group to develop a recommendation to create a new multilateral instrument or model provisions – such proposals would contribute to the international community anything that cannot otherwise be accomplished through domestic action, participation in an existing multilateral instrument, technical assistance, and greater police-to-police cooperation. Given widespread agreement on the specific core offenses of cybercrime, and the existence of robust practice and procedures in most countries for international cooperation in criminal matters, it seems clear that negotiations on a new global

[32] Draft Study (2013), p.197.

instrument or model provisions would require substantial time and resources that would inevitably be spent on debate over fundamental legal and constitutional differences, rather than cybercrime itself. Meanwhile, prosecutors, investigators, judges, and legislators – not to mention actual victims of cybercrime – would in turn receive diminished attention or support from national authorities or the international community.

The world already has multiple international legal frameworks and operational networks that can effectively combat cybercrime; a growing number of countries have substantive expertise in cybercrime and domestic law enforcement and criminal justice reform to address it; and a vast majority of developing countries want more assistance for law enforcement and criminal justice in this field. It would be unfortunate if repeated references in the Draft Study to a new global instrument distract countries from a more appropriate focus on improving their internal capacity to permit them to strengthen their domestic security and engage fully as equal and effective partners in the fight against cybercrime.