United Nations CTOC/COP/WG.3/2024/2

Conference of the Parties to the United Nations Convention against Transnational Organized Crime

Distr.: General
22 March 2024

Original: English

Working Group on International Cooperation
Vienna, 5 and 6 June 2024
Item 2 of the provisional agenda*
The role and impact of technology with regard to international cooperation in criminal matters: opportunities, challenges and capacity-building needs

The role and impact of technology with regard to international cooperation in criminal matters: opportunities, challenges and capacity-building needs

Background paper prepared by the Secretariat

I. Introduction

1. The present background paper was prepared by the Secretariat to facilitate the discussions under item 2 of the provisional agenda for the fifteenth meeting of the Working Group on International Cooperation. It presents an overview of legal and practical considerations, as well as an analysis on opportunities, challenges and capacity-building needs, pertaining to the role and impact of technology with regard to international cooperation in criminal matters.

2. The matter has been gaining prominence both in practice and in different policy-making intergovernmental forums in recent years. Indeed, technology offers efficiencies and increased capabilities for the prevention, detection, investigation and prosecution of crime, through, for example, digital case management systems and strengthened international cooperation in criminal matters and networking for secure transmission of information.

3. Moreover, from a policymaking perspective, since 2016, the Conference of the Parties to the United Nations Convention against Transnational Organized Crime has encouraged States parties to make the fullest and most effective use of available technology to facilitate cooperation between central authorities.[1] The Working Group on International Cooperation itself suggested at its fourteenth meeting in September 2023 three pertinent subtopics for further discussion, as follows:[2]

(a) The electronic transmission of international cooperation requests;

(b) The use of videoconferences, especially with regard to extradition;

* CTOC/COP/WG.3/2024/1.
[1] Conference resolution 8/1.
[2] See the report on that meeting, CTOC/COP/WG.3/2023/4, para. 44.

(c) The development of curricula for training practitioners on extradition and mutual legal assistance.

4. The above subtopics are among the issues to be examined below, together with other relevant implications and parameters of the involvement of technological innovations in the field of international cooperation in criminal matters.

II. Legal and practical considerations regarding the role and impact of technology with regard to international cooperation in criminal matters

A. Use of artificial intelligence

5. The advent of artificial intelligence (AI) holds great potential to improve efficiency in criminal justice matters, both domestically and across borders. Criminal justice and law enforcement structures are undergoing digital transformation, and AI, as a set of different technologies, has an important role to play in assisting competent authorities operate more effectively.

6. Predictive policing is a characteristic example of the impact of AI on the administration of justice: by using algorithms that process enormous quantity of data, an increasing number of law enforcement authorities have adopted software to analyse statistical data, recognize connections between various activities and cases and even predict where the next threat will emerge.[3] In terms of evidence gathering, AI systems can be of great value to law enforcement authorities, even beyond predictive policing. Analysing, for example, DNA or social media profiles produces large amounts of complex data in electronic format, which may contain useful patterns that human analysis could not be able to grasp. AI-backed tools can also be used to identify persons by means of facial recognition software. Further, AI can help in locating events and places: video, photos, satellite images and other data are triangulated to verify events in a specific time and place. While, in that case of verification of events, most of the analysis is carried out by humans, substantial portions of it could be automated or enhanced by machine learning in the future.

7. While new approaches and solutions to evidentiary matters are needed at the national level, the situation becomes even more complex in cross-border settings and therefore it is important to assess the international implications of the use of AI and related challenges for judicial cooperation. Cross-border exchange of evidence, especially from the perspective of the admissibility and use of evidence in a State other than the one in which it was gathered, has always represented a critical issue of international cooperation in criminal matters. Additionally, the relatively new challenges linked to electronic evidence add a further note of complexity.

8. Against this backdrop, it is an open question whether the existing instruments of cooperation in criminal matters can ensure exchange, admissibility and use of AI-related evidence in a satisfactory way. If each country ends up regulating the issue of AI and criminal evidence according to its own principles, rules and perhaps even technical standards, the existence of different regimes may hamper judicial cooperation, so that one may wonder whether a coordinated approach on the international level would be more appropriate.

9. As in any other case where AI systems may be used, however, the positive effects of the new technologies should not be forgotten. It is worth mentioning that, while it brings international cooperation into uncharted territories, AI could also help national authorities to deal more efficiently with requests for cooperation. According to UNICRI and INTERPOL, one example of possible future use of AI and robotics

[3] A/CONF.234/11, para. 72.

consists precisely in automation of processes with a view to autonomously researching, analysing and responding to requests for international mutual legal assistance.[4]

10. One of the most obvious cases of the use of AI in the context of judicial cooperation is that of automated document processing. Such processing normally consists of at least two components: computer vision for optical character recognition and natural language processing for document analysis and classification. Automated document processing systems may address business needs such as the conversion of scanned paper documents, PDFs and images into searchable and editable documents; the processing of high volumes of standardized documents; and the classification of documents and creation of searchable archives.[5]

11. Another application of AI that is highly relevant in cross-border collaboration is machine translation. There is a wide range of machine translation use-cases that can apply in the context of cross-border judicial cooperation, including in the work of joint investigative teams. One of the most common challenges that members of joint investigative teams face is the need to communicate in multiple languages and analyse evidence in multiple languages. In practice, this often results in the need to translate large amounts of materials, frequently containing specialist terminology or using less common languages. Even if machine-translated documents cannot be used as evidence, machine translation can at least provide a quick overview and indication of which parts of the documents might be the most important and thus the most in need of being officially translated.

12. The implementation of automated translation tools in the workflow of joint investigative teams may significantly improve performance by reducing time spent on translating evidentiary documents and making evidence more directly accessible to the team. Sworn translation will still be necessary to ensure the admissibility of translated evidence in court. However, automated translation can deliver major value at the stage of investigation and significantly reduce the time and costs for sworn translation, considering that only post-editing will be necessary in most cases, instead of translation.[6]

13. An additional application that may be relevant in the context of cross-border criminal justice cooperation is the use of automated text summarization systems. Text summarization systems are useful in applications where large amounts of information need to be processed in a limited amount of time, in particular in situations where processing of such information by humans is not feasible and where precision is not crucial.

14. Text summarization solutions are largely based on two techniques: extraction and abstraction. Extractive summarization produces summaries by selecting a subset of sentences from the original text using statistical methods. Abstractive text summarization relies on machine learning methods, with the aim of producing human-readable summaries of text containing the most relevant information.[7]

15. Even though summarization solutions can help organizations deal with large volumes of textual information, such as seized documentation, automated summarization cannot match human performance and can only help to provide a high-level and quick understanding of the content of documents, thus making the information more accessible for in-depth human analysis. In any case, documentation used for evidence will need to go through human verification and analysis. Although significant advances have been made over the past two decades in developing text summarization systems, today there are no one-size-fits-all solutions. However, there

[4] UNICRI Centre for Artificial Intelligence and Robotics and INTERPOL Innovation Centre, “Artificial Intelligence and Robotics for Law Enforcement” (2019) available at ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW ENFORCEMENT_WEB_0.pdf (unicri.it), p. 10.

[5] Artificial intelligence supporting cross-border cooperation in criminal justice, Joint report prepared by eu-LISA (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice) and Eurojust, 2022, pp. 16–17.

[6] Ibid., p. 18.

[7] Ibid., p. 19.

are increasing attempts to combine extractive and abstractive techniques to improve the quality of the summaries produced.

16. Despite the importance of textual evidence in criminal investigations, the available evidence is often not limited to text and contains a wide range of other media, including images, video and audio or voice media. The basic enabling technologies in the forensic analysis of visual media (images and video) are exactly the same as those used for facial recognition technology by border control authorities or law enforcement. Therefore, biometric identification algorithms can be relatively easily implemented in forensic video and image analysis systems. Similar technologies can be used to identify specific objects or assess the authenticity of video recordings or images (e.g. identification of deep fakes).

B. Streamlining case management systems and digitalization efforts

17. Many jurisdictions around the world have adopted digital case management systems to streamline administrative processes, reduce paperwork and expedite case management within their justice systems. Automated workflows, electronic filing systems and online document management tools can enhance efficiency and productivity for judicial institutions and legal practitioners. Moreover, the collection and analysis of data generated by digital technologies enable authorities to gain insights into case trends, case processing times and resource allocation needs. Data-driven decision-making can inform policy development, improve resource management and enhance the effectiveness of related interventions.

18. Case management in central authorities obviously reflects progress, advancements or shortcomings in the entire criminal justice institutional mechanisms of Member States, according to the varying levels of capacity. In many countries, where records continue to be kept in hard copies, searching those records and providing the relevant documents to a requesting country can be a daunting task. In countries on the other end of the spectrum, modern technology permits the use of electronic platforms for managing incoming and outgoing mutual legal assistance requests or the compilation of statistical data about cases and trends.[8]

19. Case management systems are essential for the efficiency and effectiveness of central authorities to adequately address the increasing need for enhanced international cooperation. The existence of dedicated structures or units within the central authorities to deal with the increasing volume and complexity of work relating to new and sophisticated forms of crime could be a step towards addressing the growing backlog of cases. Further, the use of statistics can facilitate more efficient case management monitoring and the realignment of resources accordingly.

20. Automated document processing can be an integral part of a case management system, supporting not only prosecutors and administrative staff involved in criminal investigations, but also authorities involved in international cooperation in criminal matters, with back-office functions relating to document processing. Automated systems can effectively extract the data necessary to classify the document and register it as relevant to a specific case, thus significantly reducing the need for manual document processing. Such automation could be useful for the creation of case information forms, which are used to collect, store and access information in support of authorities with relevant knowledge, experience and best practices.

21. The recent coronavirus disease (COVID-19) crisis and its impact on judicial cooperation in criminal matters highlighted the need for further digitalization of justice. An interesting initiative geared towards digitalization of international cooperation is taking place in Central Asia. Within the framework of the Judicial Cooperation Network for Central Asia and Southern Caucasus (CASC Network), the Global Programme on Criminal Network Disruption and the United Nations Office on Drugs and Crime (UNODC) Regional Office for Central Asia are implementing a

[8] A/CONF.234/11, para. 66.

project entitled “Digitalization of international legal cooperation processes in Uzbekistan”. The project aims at enhancing the technical capacity of the central authority of Uzbekistan by establishing a secured electronic platform for digital transmission of international judicial cooperation requests. It will contribute to the advancement of international cooperation in criminal matters at the regional and international levels.

22. Moreover, the aforementioned project will contribute to improving the effectiveness of tracking international cooperation requests, both incoming and outgoing, by developing a smart database. The digital solution will advance information collection and segregation, enabling the effective analysis of trends and contributing to effective criminal justice responses to transactional organized threats. The initiative will be supported by the development of legal and policy tools and capacity-building activities for the central authority’s personnel.

C. Videoconferencing

23. The use of videoconferencing has emerged as a priority in the field of international cooperation in criminal matters as time- and cost-saving tool to provide viva voce evidence in cases where it is impossible or undesirable for a witness to travel. It is permissible in most States and was further spurred during the COVID-19 pandemic.[9]

24. In cross-border settings, communication between judicial authorities of different Member States is crucial, and videoconferencing is one possible way of simplifying and encouraging such communication. The use of videoconferencing equipment provides courts with greater flexibility as to when and how witnesses or experts from other States can give evidence.

25. Videoconferencing technology used to be expensive, but costs have followed a decreasing trend over the years. The experience which countries have gained using videoconferencing during the COVID-19 crisis, combined with the decreasing cost and increased availability of various videoconferencing systems, has enabled competent authorities to deploy videoconferencing more effectively than ever before. Moreover, the use of videoconferencing, particularly in cross-border cases, avoids spending money on the transportation of witnesses, inmates or experts. On the other hand, on-site inspections by the court and the related costs can be avoided too, as the judges do not need to move from the courtroom. Moreover, accommodation and witness protection abroad become less necessary and related costs can be saved.[10]

26. The feedback from many professionals shows that the use of videoconferencing has grown as it proves its value in being a reliable, efficient and cost-saving tool, not only for the taking of testimony of remote witnesses, but also for a wide range of other uses such as training, communication or education.

27. In the field of international cooperation in criminal matters, relevant multilateral instruments provide for videoconferencing in their mutual legal assistance provisions. Of relevance, in this regard, are article 18, paragraph 18, of the United Nations Convention against Transnational Organized Crime and article 46, paragraph 18, of the United Nations Convention against Corruption. The *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* also reflect a set of points that can be taken as guidance to ensure that due process standards are in place when conducting hearings with witnesses heard by videoconference.[11]

[9] E/CN.15/2024/7, para. 21.
[10] UNODC, Manual on Videoconferencing: Legal and Practical Use in Criminal Cases, 2017, p. 16.
[11] *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations publication, Sales No. E.06.V.5), p. 199.

28. At the regional level, reference can be made to the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 2001 (article 9);[12] the Ibero-American Convention on the Use of Videoconferencing in International Cooperation between Justice Systems and its Additional Protocol Related to Costs, Linguistic Regime, and Submission of Requests, adopted on 3 December 2010; the ECOWAS Protocol on the Fight against Corruption of 2001 (article 8);[13] the 2008 Convention on Mutual Legal Assistance and Extradition against Terrorism signed by the French Speaking Countries of Africa (article 29); the Chisinau Convention on Legal Assistance and Conflicts of Law in Matters of Civil, Family and Criminal Law of 2002 (articles 6 and 105); and the Scheme Relating to Mutual Legal Assistance in Criminal Matters within the Commonwealth (section 14).[14]

29. Within the European Union context, cross-border videoconferences, in particular for conducting witness, expert or victim hearings, can be carried out in accordance with legal instruments such as the following: the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (article 10);[15] the Council Directive relating to compensation to crime victims (article 9 (1));[16] the Council Framework Decision on the standing of victims in criminal proceedings (article 11 (1));[17] and the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (article 24).[18]

30. In terms of soft law standards, the Council of Europe Guidelines on videoconferencing in judicial proceedings[19] provide a set of key measures that States and courts should follow to ensure that use of videoconferencing in judicial proceedings does not undermine the right to a fair trial as enshrined in article 6 of the European Convention on Human Rights and meets the requirements of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

31. Moreover, the VII Specialized Meeting of Public Ministries of MERCOSUR and Associated States, held on 29 May 2009 in Asuncion, approved the “Asuncion Guide on the Use of Videoconferencing in Criminal Proceedings”. The guide establishes the need to harmonize legislative, technical and operational guidelines for the use of videoconferencing. It also includes a recommendation that each prosecution office should designate a national coordinator for the use of videoconferencing, who acts as the contact point for the requesting countries and as a facilitator for the rest of the national institutions to guarantee the necessary coordination for the success of the videoconference.

32. In practical terms, the videoconference tool has also been used in cases linked to extradition processes. From the perspective of the person under investigation, who can also be, at a certain stage, a person sought for purposes of extradition, videoconferencing offers multiple advantages. A hearing by videoconference could be an effective, proportionate and less intrusive measure than extraditing the accused or, in the European Union context, issuing a European arrest warrant. This is particularly the case at initial stages of the investigation, when the suspect’s presence before the judicial authority is not yet absolutely necessary, for example, at an early stage of the proceedings. For a suspect under investigation located in a different country from which the investigation is being carried out, videoconferencing can be

[12] ETS No. 182.
[13] ECOWAS_Protocol_on_Corruption (cartercenter.org).
[14] P15370_13_ROL_Schemes_Int_Cooperation.pdf (production-new-commonwealth-files.s3.eu-west-2.amazonaws.com).
[15] *OJ C 197*, 12.7.2000, pp. 1–23.
[16] *OJ L 261*, 6.8.2004, pp. 15–18.
[17] *OJ L 315*, 14.11.2012, pp. 57–73.
[18] *OJ L 130*, 1.5.2014, pp. 1–36.
[19] Adopted by the European Commission for the Efficiency of Justice (CEPEJ) in June 2021. Available at 151221GBR_Guidelines videoconferencing.pdf.

a more convenient method of testifying and exercising his or her defence without the suspect needing to travel to the country in which the process is being held. Through videoconferencing, the suspect is allowed to exercise his or her right to counsel by testifying or refraining from testifying, thereby allowing the process to continue its natural course and offering the suspect under investigation the possibility of remaining linked to the process without the risk of him or her being considered in default.

D. Electronic transmission of international cooperation requests

33. Technology played an important role in overcoming restrictions posed by the COVID-19 pandemic in the field of international cooperation in criminal matters. As an example, the conditions created by the pandemic have led to greater support for the idea that international cooperation requests can be sent and answered in a safe, timely, agile and valid manner using electronic means.[20]

34. The use of technologies such as the electronic transmission of requests in extradition and other proceedings, the use and acceptance of electronic signatures and the paperless administration of work in central and other competent authorities more generally was also encouraged by the Conference of the Parties to the Organized Crime Convention in its resolution 11/1.[21] In particular, the Conference encouraged Member States to allow flexibility regarding the acceptance of official documents bearing electronic or digital signatures.[22] Member States were also encouraged to further strengthen their ability to use electronic means for the transmission of mutual legal assistance requests and for seeking, in response to such requests, clarifications and acceptance of relevant materials in electronic form, in accordance with the fundamental principles of their domestic law, including with a view to improving their capabilities in the post-COVID-19 era.[23] Considering the variations in the acceptance and availability of technology and communications based on it, implementing a relatively harmonized standard of electronic communication would already be a major endeavour.

35. At the sixth meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held from 27 to 29 July 2020, the need to modernize, streamline and expedite mutual legal assistance practice through the electronic transmission of international cooperation requests was emphasized. In this context, it was stressed that central and other competent authorities could transmit, by email, requests for both formal and interinstitutional assistance, as well as preservation requests, using “24/7” networks.[24]

36. An increasing number of central authorities worldwide accept email for the transmission of mutual legal assistance requests. As reported in a UNODC study on the impact of the COVID-19 pandemic on international cooperation in criminal matters: challenges encountered, good practices and lessons learned in the aftermath of the pandemic (soon to be published), since the end of the pandemic, central authorities have been generally more inclined to engage electronically, including to receive and send mutual legal assistance requests electronically and with electronic signatures than before the pandemic. There is also a more prominent shift to the electronic submission of evidence.

37. From a normative perspective, article 18, paragraph 14, of the Organized Crime Convention stipulates that requests for mutual legal assistance shall be made in writing or, where possible, “by any means capable of producing a written record […] under conditions allowing that State Party to establish authenticity”. A similar

[20] CTOC/COP/WG.3/2021/2, paras. 23ff.

[21] Resolution 11/1, annex I, “Impact of the coronavirus disease (COVID-19) on international cooperation in criminal matters: a one-year overview”: Endorsement of recommendations of the Working Group on International Cooperation, para. (r).

[22] Ibid., para. (v).

[23] Ibid., para. (w).

[24] UNODC/CCPCJ/EG.4/2020/2, para. 32.

provision is contained in article 46, paragraph 14, of the Convention against Corruption. According to article 4, paragraph 9, of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, "requests for mutual assistance and any other communications […] may be forwarded through any electronic or other means of telecommunication provided that the requesting Party is prepared, upon request, to produce at any time a written record of it and the original. However, any Contracting State, may by a declaration addressed at any time to the Secretary General of the Council of Europe, establish the conditions under which it shall be willing to accept and execute requests received by electronic or other means of telecommunication".

38. The newly updated UNODC Model Law on Mutual Assistance in Criminal Matters,[25] refers to the conditions for electronic transmission of electronic evidence. Section 29 of this Model Law refers to the need to ensure: (a) the security and integrity of the evidence; (b) the identification, authentication and verification of the sender and recipient; and (c) the compliance with any applicable domestic data protection/data privacy laws. These requirements or criteria must be envisaged when developing technological capabilities in the field of mutual legal assistance.

39. Email security capabilities vary from one central authority to another, with some countries possessing their own public administration domain, with state-of-the art encrypted technology, while others, at the opposite end of the spectrum, utilizing free email domains, with the corresponding lower levels of security. It would be recommended to alleviate the digital divide that persists across central authorities for mutual legal assistance by supporting the establishment of secure email communication channels.

40. Ensuring that international cooperation is adjusted to the challenges and opportunities of the new digital era has gained significant importance in recent years. In this regard, priority should be accorded to the need to advance from physical to electronic communication, using secure platforms equipped with electronic certification and digital signature, that guarantee data protection, ensure the legitimacy of the parties involved and allow the documentation to have full legal effect in judicial procedures.

41. The Ibero-American Network for International Legal Cooperation, IberRed, has a secure communication system called "Iber@", through which international legal assistance requests can be sent. The Treaty Relating to the Electronic Transmission of Requests for International Legal Cooperation among Central Authorities of 2019, known as the Medellín Treaty, does not oblige the parties to use "Iber@" for the transmission of requests for international judicial cooperation, but once the central authority receives the request through it, subsequent communications relating to its execution shall be sent to the issuing central authority by the same means, unless the nature of the request or a supervening situation makes this inadvisable, in which case the sender must be informed.

E. Role of technology in promoting judicial cooperation and information exchange

1. Secure communication and information exchange in the context of judicial cooperation

42. The importance of quick responses to requests for international cooperation in criminal matters is widely acknowledged. Article 18, paragraph 13, of the Organized Crime Convention provides for the direct communication among central authorities and the transmission of requests to them. From a policy perspective and since the early phases of its work, the Conference of the Parties to the Organized Crime Convention has devoted particular attention to ways and means of using technology

[25] Model_Law_Mutual_Legal_Assistance_2022.pdf (unodc.org).

for ensuring better communication among central authorities involved in international cooperation in criminal matters.[26]

43. At the regional level and within the context of the European Union, Eurojust has been called to create "Cross-Border Digital Criminal Justice", a fast, reliable and secure information technology infrastructure that would enable national prosecution authorities to interact with their counterparts. Following the December 2018 Justice and Home Affairs Council Conclusions, the European Commission launched the Digital Criminal Justice project. The objective of this project is to shape a vision to design and implement a host of digital measures for the cross-border cooperation in criminal matters. According to the Cross-border Digital Criminal Justice Final Report (2020) of the European Commission, among the categories of business needs identified in the context of this project was the necessity to securely communicate and exchange information via digital means.[27] This requires solutions to allow stakeholders to communicate in a secure way, including sending and receiving sensitive and confidential data. Moreover, it was found that in any information technology system landscape with the need of information exchange across different systems and components, interoperability (the ability of computer systems or software to exchange and make use of information) must always be ensured, alongside the compatibility of the security measures being implemented.[28]

44. Secure communication platforms may offer solutions in practice to facilitate timely and efficient communication between practitioners and promote exchange of information among authorities involved in international cooperation in criminal matters, including follow-up on the execution of international cooperation requests. In the day-to-day functioning of competent authorities, the consistent use of emails as a means of rapid communication has proved very useful. However, secure communication platforms provide more features for sharing information among the practitioners. Apart from sharing texts, files or images, secure communication platforms also allow practitioners to send audio messages, make audio or video calls, and check whether the recipients have received or read the messages. The last feature, in particular, would help the practitioners to track and follow up on their requests and reduce delay in responses.

45. In view of the increasing needs of practitioners to engage in secure communication among themselves, UNODC is exploring the feasibility of putting in place a secure communication platform to facilitate direct communication and informal exchanges among central authorities dealing with mutual legal assistance requests. One possibility under examination is to build on the example of the secure communication platform of the GlobE Network (see paragraph 53 for further information) and engage the services of the same external vendor for the development of a similar application to be used as a secure communication platform by central authorities involved in mutual legal assistance.

46. At the time of drafting, the secretariat was testing the technical features of the application and their adaptability to the purposes of promoting communication in the field of mutual legal assistance. What is also under examination is how to connect the application with the online Directory of Competent National Authorities in the sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

2. Facilitating the exchange of information in the context of law enforcement cooperation

47. Article 27, paragraph 3, of the Organized Crime Convention calls upon States parties to endeavour to conduct law enforcement cooperation in order to respond to transnational organized crime committed through the use of modern technology.

[26] See decision 3/2, para. (u); and decision 4/2, para. (w). See also resolution 8/1, para. 6, and annex I, para. (l).

[27] European Commission, "Cross-border digital criminal justice", Final report 2020, p. 3.

[28] Ibid., pp. 3 and 51.

Further, according to article 27, paragraph 1 (a), of the Convention, States parties should take effective measures to enhance and establish channels of communication between their competent authorities in order to facilitate the secure and rapid exchange of information concerning all aspects of offences covered by the Convention.

48. In terms of the day-to-day functioning of relevant law enforcement authorities, the consistent use of emails as a means of rapid communication has proved very useful, and tools such as secure databases for the sharing of information among law enforcement authorities have been developed. According to the *Travaux Préparatoires of the Negotiations for the Elaboration of the Organized Crime Convention*, States parties will make their own determination as to how best to ensure the secure and rapid exchange of information.[29]

49. Moreover, pursuant to article 12, paragraph 1, and article 13, paragraph 1, of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime, States parties should exchange information and cooperate at the bilateral, regional and international levels to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition. Technology can help to make this cooperation and information exchange faster and more efficient. Similar provisions on information exchange are found in the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (article 10) and in the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime (article 10), subject to the scope of application of each protocol.

50. In the context of border management, single window processing helps to meet the challenge of facilitating the movement of people and goods while maintaining secure borders, as well as preventing and detecting trafficking in firearms, their parts and components and ammunition. Single window processing allows an importer or exporter to provide all necessary information and documentation to a designated host government agency through an electronic platform. The host then distributes this information to all relevant agencies, which apply risk assessment techniques to determine if the goods should be stopped for inspection. The single window approach can be combined with direct lines of communication between border agencies on opposite sides of the borders on suspicious transactions, as well as with early warning procedures that allow for the sharing of new developments requiring immediate countermeasures.[30]

51. Article 12, paragraph 4, of the Firearms Protocol requires States parties to cooperate in the tracing of firearms, their parts and components and ammunition that may have been illicitly manufactured or trafficked. Effective tracing relies on comprehensive firearms registries that provide information about the entire life cycle of a firearm: from manufacture or import to individual transactions and finally export, disposal or destruction. Integrated and digitalized firearms registries, such as the record-keeping software "goIFAR", which was developed by UNODC and can be tailored to national needs, permit the identification and tracing of a firearm in real time. Furthermore, INTERPOL has developed several information technology tools that facilitate global information exchange and cooperation between authorized law enforcement agencies, including specialized tools on firearms trafficking and firearms crime. For instance, through the INTERPOL Illicit Arms Records and Tracing Management System, to which over 180 countries have access, members can trace seized, lost and stolen firearms. Moreover, the INTERPOL Ballistic Information

[29] See *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations publication, Sales No. E.06.V.5), p. 244. See also CTOC/COP/WG.3/2023/2, para. 17.

[30] United Nations, Office of Disarmament Affairs, Modular Small-arms-control Implementation Compendium, MOSAIC, 05.60, "Border controls and law enforcement cooperation" (2018), p. 24 ff.

Network allows the sharing and comparing of ballistic data, including across borders, to determine if the same firearm was used at different crime scenes. These weapon-specific systems can be used in parallel with broader INTERPOL tools, such as the network of national central bureaus, the system of international notices and any other INTERPOL database, accessible through the I-24/7 global police communications system.[31]

52. In addition, UNODC launched in April 2022 a Knowledge Hub on Human Trafficking and Migrant Smuggling (KNOWTS), used by approximately 1,400 participants from 114 countries. Through knowledge-sharing and live events, KNOWTS facilitates the informal and interactive sharing of information between criminal justice practitioners and the strengthening of practitioners' networks. This has, in turn, facilitated the exchange of information related to specific cases and fostered cooperation in a more agile and timely manner while formal requests for cooperation are implemented.

53. The Global Operational Network of Anti-Corruption Law Enforcement Authorities (GlobE Network) was established in June 2021 by UNODC to facilitate informal cooperation and to address the lack of a truly global network for anti-corruption law enforcement authorities. The Network has an online one-stop hub of the Global Operational Network of Anti-Corruption Law Enforcement Authorities (GlobE Network) to provide a forum for cooperation, which includes a secure platform for confidential communication among Network members. GlobE Threema, a secure corporate communication solution, was rolled out in 2022 exclusively for GlobE practitioners free of charge. Access to GlobE Threema is granted to designated representatives of the GlobE Network members.[32]

F. Fostering international cooperation through technological innovations and tailor-made tools

54. As in any other fields or industry, practitioners engaged in international cooperation in criminal matters experience in their daily work the benefits of an array of technological applications. UNODC has undertaken action to promote international cooperation, including through tailor-made tools and technological innovations, including the following: SHERLOC and its secure module known as "RevMod", which was specifically built to facilitate the conduct of country reviews within the framework of the Mechanism for the Review of the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto; the UNODC Directory of Competent National Authorities; and the redeveloped version of the Mutual Legal Assistance Request Writer Tool.

55. Data driven systems with search engine capabilities, such as the aforementioned directory, enable the identification in a secure and authenticated form, of the contact details of central and competent authorities around the world. Data analytics technology can be integrated and implemented in the Directory of Competent National Authorities to produce statistical visualisations for the convenience of, and further use by, the users of the directory.

56. The UNODC Mutual Legal Assistance Request Writer Tool is a digital tool that UNODC has developed to assist criminal justice practitioners, particularly officers of central authorities involved in mutual legal assistance, in drafting expeditiously mutual legal assistance requests. In line with applicable security standards, the Tool is currently being upgraded with a view to enhancing its compliance with United Nations security standards. The upgraded tool will enjoy a more secure configuration and integration into existing network infrastructure and will be embedded into the password-protected UNODC Directory of Competent National Authorities. This, will,

[31] UNODC, *Technical Guide to the Implementation of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms*, pp. 101 ff.

[32] CAC/COSP/EG.1/2023/2, para. 39.

in turn, result in a situation where both tools will enjoy a higher degree of synchronization and interoperability.

G. Technology and mutual legal assistance to obtain or preserve electronic evidence

57. As electronic evidence can be obtained through a third party (communication service providers), access to data from different kinds of service providers has become crucial for successful cross-border investigations in recent years. For that reason, it is extremely important to forge partnerships between communication service providers and law enforcement agencies.[33]

58. A thorough reflection on the needs and limits of gathering electronic evidence from those private actors could be part of a broader discussion on the role of technology in enforcement and on challenges created by constant technological developments, including the gathering and examining of evidence by means of the Internet of things and AI.

59. The stage and complexity of the investigation or criminal proceedings at the time when a request for assistance is received, as well as the extent to which the measures needed to afford such assistance involve the handling of electronic data or evidence, determine the need for the use of specific technologies. In the case of the preservation, disclosure and production of stored computer data, the use of dedicated online portals for law enforcement cooperation are known to be the fastest and most efficient ways to contact communication service providers. These online portals are usually enabled by the communication service providers, or in some instances, they are offered by third-party companies specialized in streamlined communication between companies and law enforcement, regulators and other government agencies. Purpose-built secure law enforcement communication portals represent more robust security solutions, in comparison to traditional manual modes of communication or of software that have not been built with this purpose in mind and may, as a result, be more susceptible to vulnerabilities and risks.[34]

60. The management of electronic evidence requires the same secure chain of custody as physical evidence. However, the storage and preservation of electronic evidence assets present multiple unique challenges to cross-border evidence operations. Sustainable evidence operations must balance the scope and scale of electronic evidence management and keep up with technological advancements to accommodate the changing needs in this field. Almost all sustainable evidence operations leverage available technologies to increase operational efficiency and effectiveness. Implementation and adoption of technology and electronic evidence standards and practices promote a stable organizational baseline for sustainable evidence management.

61. Storing evidence in conditions that preserve the forensic integrity and original condition of the item is a key principle of evidence management. Efficient evidence storage operations utilize organization and filing systems in concert with appropriate storage methods and technology to maximize available facility space. The use of technological solutions for effective evidence storage operations facilitates the location and retrieval of any evidence item in a timely manner. From a data protection perspective, retention periods need to be in place so that the data are not kept for longer than is needed to fulfil the purpose for which they were processed and stored.

[33] E/CN.15/2022/6, para. 7.

[34] For an overview of the general practices developed by international service providers in responding to overseas government requests for data, see the UNODC DATA DISCLOSURE FRAMEWORK (DDF), available at the SHERLOC Electronic Evidence Hub.

H. Human rights considerations

62. Technology-based tools can be useful entry points for addressing crime-related threats. However, caution is needed in the specific application of these tools to ensure responsible and ethical use and avoid unintended consequences. This is particularly important given that many of the present and future technologies may have serious implications for personal privacy and civil liberties.

63. Notwithstanding the benefits brought by technology-based tools in the field of international cooperation in criminal matters, such tools entail a number of potential risks, such as opaque decision-making, different types of discrimination, the intrusive nature of their use and challenges to the protection of privacy and personal data. These potential risks are aggravated in the sectors of law enforcement and criminal justice, both domestically and in the sphere of international cooperation, as they may affect the presumption of innocence and the fundamental rights to liberty and security of the individual and to an effective remedy and fair trial.

64. As an example, the use of artificial intelligence and machine learning algorithms in decision-making processes raises ethical and legal concerns regarding transparency, accountability, bias and fairness. Ensuring that AI systems operate in accordance with human rights principles and do not perpetuate discrimination or reinforce existing inequalities is a complex challenge. When the outcome of algorithmic calculations by AI systems is used, in particular as evidence before a criminal court, the fundamental right to a fair trial may be violated at least for two different reasons. First, the algorithmic processes that analyse the data and end up providing public authorities with a given piece of evidence are often obscure. Insofar as individuals in a legal process are unable to understand and contest, even with the help of legal counsel, complex algorithmic systems used to process evidence alleged to relate to them, there is a significant threat to due process rights. Second, and consequently, if investigations are based on AI techniques, the defendant should be in a position to understand how evidence has been gathered. Otherwise, the use of AI-related evidence poses a risk to the principle of equality of arms.

65. The General Assembly adopted, for the first time, a landmark resolution on the promotion of "safe, secure and trustworthy" AI systems that will also benefit sustainable development for all.[35] The Assembly called upon all Member States and other stakeholders "to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights". The Assembly also reaffirmed that "the same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence systems".

66. The importance of compliance with procedural safeguards for the admissibility in court of the evidence obtained through special investigative techniques, including those involving the use of modern technology, needs to be acknowledged. In most jurisdictions, the process of gathering evidence requires strict adherence to a number of safeguards against potential abuses of authority, including judicial or independent oversight of the use of those techniques and observance of the principles of legality, subsidiarity and proportionality.[36] This is tightly linked to the positive obligation of a State to have in place laws, regulations and procedures to enable, for the sake of legal certainty, the proper administration of justice and protection of human rights and fair trial standards.

67. Moreover, the conditions and safeguards for the collection and use of electronic evidence predominantly require judicial or other independent oversight to delineate limits on the procedures, processes, methods and tools used to collect, acquire, preserve and analyse electronic evidence. Consequently, priority should be accorded

[35] General Assembly resolution 78/265. At the time of writing, the resolution document had not yet been issued. See the draft resolution (A/78/L.49).

[36] CTOC/COP/WG.3/2020/3, para. 66.

to the need for procedural legislation granting powers to competent law enforcement authorities to gather electronic evidence effectively while observing confidentiality, privacy, human rights, due process and other legal safeguards.[37]

68. In sum, a balanced approach is needed to find solutions in cases where technology and privacy or other human rights seem to be on a collision course.[38] The implementation of such solutions in the judicial and law enforcement fields cannot be considered as a purely technical challenge. The development and deployment of AI-driven solutions in particular should be evaluated with special care in order to avoid situations where fundamental rights and freedoms of individuals are negatively affected and persons are subjected to various forms of discrimination, limitations of rights or unfair treatment.

69. Ensuring the protection of human rights in the development and use of digital technologies within the administration of justice requires multidisciplinary and multisectoral approaches that integrate legal and technical safeguards, as well as oversight mechanisms to ensure compliance with fundamental rights and freedoms. The undertaking of human rights impact assessments conducted prior to the design and implementation of digital technologies is an essential component of responsible and accountable governance in the development and use of digital technologies within the administration of justice. Such assessments help to identify and analyse potential risks and impacts of the digital technologies on human rights, including privacy, fair trial, non-discrimination and access to justice. Furthermore, continuous monitoring and evaluation mechanisms, which are established at later stages of the digital technology implementation process within the administration of justice, track the performance, impact and outcomes of digital technologies in relation to human rights standards and principles.

I. Capacity-building and technical assistance needs

70. The adoption of digital technologies necessitates training and capacity-building efforts to equip authorities involved in international cooperation in criminal matters with the necessary skills and knowledge to effectively utilize these technologies. The lack of technological equipment leads to disparities in access to, and proficiency with, technology among countries. The discrepancy in skill sets among practitioners presents a barrier to meaningful engagement in international cooperation through technological channels, underscoring the need for equitable capacity-building efforts. Moreover, proactive measures need to be taken to address the digital divide and ensure equitable access to technology through enhancing the skills of practitioners.

71. Resistance to change and the need for ongoing technical support are common challenges during the transition to digital platforms. Access to, and proper use of, technology by authorities involved in international cooperation in criminal matters require financial resources, training and expertise. Those authorities must evolve with changes within their environment with a view to reducing the opportunities presented to offenders by technological advances. Being left behind makes it impossible for international cooperation mechanisms to effectively address transnational organized crime that exploits advancements in technology.

72. Specific techniques and technology have become essential for international cooperation in criminal matters to combat cyber organized crime. Although leveraging specialized software, employing open-source intelligence techniques and utilizing advanced hardware undoubtedly enhance and accelerate investigations, it remains imperative to acknowledge the challenges and gaps that still need to be addressed. Moreover, the misuse of technology exacerbates challenges in fostering international cooperation, emphasizing the necessity for holistic strategies to mitigate such risks and promote responsible use of technological tools in collaborative endeavours.

[37] CTOC/COP/WG.3/2023/2, para. 70.
[38] A/CONF.234/11, para. 78.

73. Member States need to promote, in cooperation with UNODC and other international organizations, technical assistance and training to enhance the skills of practitioners and central authorities in the use of technology to expedite international cooperation.[39] One of the recommendations of the Kyoto crime congress workshop on current crime trends, recent developments and emerging solutions, in particular new technologies as means for and tools against crime was that Member States should seek to streamline international cooperation in criminal matters through the use of technology and innovative tools by practitioners and central authorities that are equipped and empowered to fully benefit from such technology and tools.[40]

74. The Global Initiative on Handling Electronic Evidence was launched by UNODC, together with Counter-Terrorism Committee Executive Directorate and the International Association of Prosecutors, in 2017. It aims at enhancing the capacity of: (a) law enforcement authorities to identify, collect, acquire and preserve the electronic data needed to investigate terrorism and other serious offences; (b) prosecutorial and judicial authorities to use those data as evidence in court; and (c) central and competent authorities to handle and exchange those data across borders and jurisdictions, without jeopardizing their admissibility and probative value in court.[41]

75. In May 2021, the Global Initiative launched the Electronic Evidence Hub, a one-stop shop for various practical tools specifically tailored to the needs of law enforcement, judicial and central authorities.[42]The Hub includes a range of resources, such as the first and second editions of the Practical Guide for Requesting Electronic Evidence across Borders, the Service Providers Mapping, the Train-the-Trainer Module and the Catalogue of Cross-Border Exercises.[43]

76. The Global Programme on Cybercrime is mandated to assist Member States in their fight against cybercrime through capacity-building and technical assistance. Technical assistance and international cooperation play pivotal roles in facilitating essential information-sharing, fostering the exchange of best investigative practices and cultivating expertise within the realm of cyberspace.

77. Through its six areas of intervention (digital evidence, cyber investigations, virtual assets, online child sexual abuse, prevention and digital forensics), the Global Programme on Cybercrime, works with a wide range of actors, including the justice sector, ministries of education, communication service providers, technology companies and private companies. In this regard, the Global Programme has supported Member States in increasing their knowledge and understanding of digital evidence and how to request it from technology companies and communication service providers. In the area of online child sexual abuse and exploitation, the Global Programme has promoted and provided the use of specialized software. This technology not only expedites criminal investigations, but also ensures the secure exchange of data in cases involving child sexual abuse material. In the field of digital forensics, the Global Programme has spearheaded the establishment of digital forensic laboratories and provided comprehensive training on extracting digital evidence from cloud-based sources, equipping law enforcement professionals with the necessary skills to navigate digital evidence effectively.

78. Under the strengthening transregional action and responses against the smuggling of migrants (STARSOM) initiative, which enabled countries along the transcontinental smuggling routes from South Asia to North America to work more closely together to effectively respond to migrant smuggling while protecting the lives and upholding the rights of the smuggled migrants, UNODC has facilitated the establishment of special units, with specific attention to training in the collection of electronic evidence, digital data mobile extraction devices, and mobile forensics or

[39] A/CONF.234/11, para. 82 (l).
[40] A/CONF.234/16, para. 192 (j).
[41] E/CN.15/2022/6, para. 25; CTOC/COP/2022/6, para. 47.
[42] Available at https://sherloc.unodc.org/cld/en/st/evidence/electronic-evidence-hub.html.
[43] CTOC/COP/2022/6, para. 48.

documenting the dynamics of smuggling. This, in turn, could contribute to the early identification and referral of migrant smuggling for investigation and prosecution in many countries.[44]

III. Conclusions and recommendations

79. The Working Group may wish to recommend that the Conference of the Parties to the Organized Crime Convention:

(a) Encourage States parties to streamline international cooperation mechanisms through the use of technology and innovative tools by practitioners and competent authorities that are equipped and empowered to fully benefit from such technology and tools;

(b) Encourage States parties to facilitate training activities for central and other competent authorities involved in international cooperation in criminal matters, as well as other practitioners engaged in such cooperation, to make effective and human rights-compliant use of the modern technologies at their disposal; and invite the secretariat, subject to the availability of resources, to develop and implement technical assistance activities in this area;

(c) Encourage States parties to monitor and understand the risks posed by the malicious use of technologies and promote ethical standards in the use of these technologies for international cooperation purposes;

(d) Encourage States parties to exchange, at forums within the framework of the Conference of the Parties to the Organized Crime Convention, information on good practices, challenges and proposals to enhance international cooperation in criminal matters through the use of technology and innovative tools.

[44] See UNODC, *The scope of transcontinental migrant smuggling from South Asia to North America*, strengthening transregional action and responses against the smuggling of migrants (STARSOM) initiative, 2023, p. 41.