United Nations A/CONF.234/11

Fourteenth United Nations Congress on Crime Prevention and Criminal Justice

Distr.: General
23 January 2020

Original: English

Kyoto, Japan, 20–27 April 2020

Item 6 of the provisional agenda[*]
International cooperation and technical assistance to prevent and address all forms of crime

Workshop 4. Current crime trends, recent developments and emerging solutions, in particular new technologies as means for and tools against crime[**]

Background paper prepared by the Secretariat

Summary

The present background paper examines the impact of technology, which is a double-edged sword: it enables crime but also contributes to its prevention, detection and suppression. Accordingly, this paper adopts a two-pronged approach to explain the emerging fundamental dualism: technology's role in finding solutions in policing, prosecutions and successful criminal justice outcomes, on the one hand; and, on the other, technology's darker role of enhancing the modi operandi of criminals and organized criminal groups. The analysis takes into account developments in specific areas and covers two aspects of a cross-cutting nature: the importance of training, interdisciplinary approaches and collaborative synergies among relevant stakeholders to gain an understanding of the current benefits of technologies and their potential in addressing future crime threats, and the necessity of giving due consideration to ethical issues and human rights safeguards in using technologies to combat crime.

[*] A/CONF.234/1.

[**] The Secretariat wishes to express its appreciation to institutes of the United Nations crime prevention and criminal justice programme network, especially the Korean Institute of Criminology and the National Institute of Justice of the United States Department of Justice, for assisting in the preparation and organization of the workshop.

I. Introduction

1. In 1997, when the United Nations International Drug Control Programme and the Centre for International Crime Prevention were merged to form the Office for Drug Control and Crime Prevention, renamed the United Nations Office on Drugs and Crime (UNODC) in 2002, an upgraded version of a chess-playing computer named "Deep Blue" became the first computer system to defeat a reigning world champion in a match under standard chess tournament time controls. At that time, despite the steady march of technological advancements, crime was still relatively "low tech" and the Internet was just starting to have an impact on society as the decisive technology of the "Information Age".

2. In a little more than two decades, the rapid growth of the Internet and information and communication technologies has enabled economic growth and broad access to vital services but has also created new opportunities for criminal activities. Criminals have become the unintended beneficiaries of new technology and globalization as those developments have enabled them to commit crimes and profit from them by exploiting transnational activities and to expand their illicit activities and businesses on digital platforms in a way that has lowered the risks, in particular the risk of detection.[1]

3. On the other hand, new and existing technologies provide new opportunities for law enforcement actions, criminal investigation and prosecution. Improving public safety and empowering law enforcement and criminal justice authorities to prevent and combat crime through technological advances may have a positive impact on achieving the goals of the 2030 Agenda for Sustainable Development, in particular Sustainable Development Goal 16.

4. In its report entitled "The age of digital interdependence", the High-level Panel on Digital Cooperation, established by the Secretary-General in 2018 to strengthen international and multi-stakeholder cooperation and contribute to the public debate on a safe and inclusive digital future for all, also highlighted the "two faces of Janus". As stated, digital technologies have proved that they can connect individuals across cultural and geographic barriers, increasing understanding and potentially helping societies to become more peaceful and cohesive. However, there are also examples of digital technologies being used to violate rights, undermine privacy, polarize societies and incite violence.[2]

5. The present background paper builds on and expands the thematic framework of workshop 4, as reflected in the discussion guide of the Fourteenth Congress.[3] This background paper is structured in separate sections, each of which reflects different angles of the same core issue: law enforcement and criminal justice authorities at the crossroads, owing to fast-paced technological innovations that not only may be conducive to effective policing and instrumental in addressing traditional shortcomings of efforts to fully enforce the rule of law but also are prone to criminal exploitation in different areas.[4]

[1] Yury Fedotov, "In just two decades, technology has become a cornerstone of criminality", *Huffington Post UK*, 23 October 2017.

[2] See United Nations, "The age of digital interdependence", June 2019, p. 17.

[3] A/CONF.234/PM.1, paras. 161–189.

[4] The use of the Internet and digital technologies for terrorist purposes, as well as issues related to cybercrime, are covered in the working paper prepared by the Secretariat on agenda item 6 (A/CONF.234/7).

II. Technologies as tools for and against crime

A. Cryptocurrencies and virtual assets

6. In recent years, cryptocurrencies and virtual assets have emerged and attracted investment in payment infrastructure built using their software protocols.[5] Users of cryptocurrencies may find them desirable for a variety of reasons, while they may also hold such assets as speculative investments. Some users seek the privacy associated with higher levels of anonymity of transactions, while others simply want to avoid the oversight and/or control of the State or banks with regard to their legal transactions.[6] Proponents of cryptocurrencies point to transaction fees that are lower than those charged by traditional banks for national currencies, although any exchange rate loss and the fees associated with cryptocurrency service providers can undercut the cost savings.[7] In locations where traditional banks are unavailable, cryptocurrencies can offer the functionality associated with traditional payment services.[8] Finally, since cryptocurrency is typically not a State currency, it can ease cross-border transactions.[9]

7. Nevertheless, many of the countries that permit the operation of cryptocurrency markets have enacted laws to prevent money-laundering, organized crime and terrorism financing,[10] although, to date, there does not appear to be large-scale use of cryptocurrencies by terrorists.[11] This trend of regulation emerged as a reaction to the frequent use of cryptocurrencies to make illegal and black-market purchases online[12] and as a payment method in cases of money-laundering, Ponzi schemes, extortion, blackmail (the threat of distributed denial of service (DDOS) attacks) and fraud.

8. The same concepts that apply to money-laundering using cash can also apply to money-laundering using cryptocurrencies.[13] Money-laundering involving cryptocurrency follows a process similar to that of traditional money-laundering but exploits technology to launder the money.[14] In addition, cryptocurrencies might be used to facilitate tax evasion.[15]

[5] Sesha Kethineni and Yin Cao, “The rise in popularity of cryptocurrency and associated criminal activity”, *International Criminal Justice Review*, 6 February 2019; Stearns Broadhead, “The contemporary cybercrime ecosystem: a multi-disciplinary overview of the state of affairs and developments”, *Computer Law and Security Review*, vol. 34, No. 6 (December 2018), pp. 1180–1196.

[6] Geoff Goodell and Tomaso Aste, “Can cryptocurrencies preserve privacy and comply with regulations?”, *Frontiers in Blockchain*, vol. 2, art. 4 (May 2019), pp. 1–20.

[7] Angela S. M. Irwin and Adam B. Turner, “Illicit Bitcoin transactions: challenges in getting to the who, what, when and where”, *Journal of Money Laundering Control*, vol. 21, No. 3 (July 2018), pp. 297–313.

[8] Ibid.

[9] Perri Reynolds and Angela S. M. Irwin, “Tracking digital footprints: anonymity within the bitcoin system”, *Journal of Money Laundering Control*, vol. 20, No. 2 (May 2017), pp. 172–189.

[10] United States, Law Library of Congress, Global Legal Research Center, *Regulation of Cryptocurrency around the World* (Washington, D.C., 2018), June 2018.

[11] Cynthia Dion-Schwarz, David Manheim and Patrick B. Johnson, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, California, RAND Corporation, 2019).

[12] Reynolds and Irwin, “Tracking digital footprints”; Monica J. Barratt, Jason A. Ferris and Adam R. Winstock, “Safer scoring? Cryptomarkets, social supply and drug market violence”, *International Journal of Drug Policy*, vol. 35 (September 2016), pp. 24–31.

[13] Chad Albrecht and others, “The use of cryptocurrencies in the money laundering process”, *Journal of Money Laundering Control*, vol. 22, No. 2 (May 2019), pp. 210–216; Rolf van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, “Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin”, *Journal of Financial Crime*, vol. 25, No. 2 (June 2018), pp. 419–435.

[14] Denis B. Desmond, David Lacey and Paul Salmon, “Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review”, *Journal of Money Laundering Control*, vol. 22, No. 3 (July 2019), pp. 480–497.

[15] Albrecht and others, “The use of cryptocurrencies in the money laundering process”; Saman Jafari and others, “Cryptocurrency: a challenge to legal system”, 10 May 2018.

9. Theft of cryptocurrency is also a growing concern.[16] Users of cryptocurrency can fall prey to scams designed to steal cryptocurrency.[17] Moreover, ransomware attacks against individuals, companies or governments often make use of extortion demands to be paid in cryptocurrency.

10. Crime involving cryptocurrencies is facilitated in environments where regulations are insufficient to permit user identification or impose sanctions, and where regulatory loopholes can be exploited. Differences in the regulations on cryptocurrencies in different countries enable users to conduct in one country an activity that is illegal elsewhere.[18]

11. A number of actions should be considered and pursued to prevent the use of cryptocurrencies for criminal purposes. Approaches to de-anonymize transactions can support deterrent and investigative functions. These may include regulations to require identifying information ("know your customer" rules)[19] or analysis of transactions using machine learning or other surveillance techniques to identify illegal transactions.[20]

12. The limited knowledge and skills for identifying or effectively investigating cryptocurrency schemes paves the way for expanded opportunities to use cryptocurrencies for the purpose of illicit activities.[21] Efforts such as those undertaken by the United Nations to provide training to investigators on cryptocurrency crime contribute to the prevention and identification of such activities.[22]

13. Issuers of cryptocurrency, regulators and law enforcement authorities are key players in hindering the use of cryptocurrency to facilitate crimes. It is important to develop a robust set of prevention and investigative techniques that can be adapted to changes in technology and the various applications of cryptocurrencies with a view to minimizing threats associated with their criminal misuse.

B. Technology and darknet markets, including drug markets

14. The Internet offers new opportunities for the illicit selling and purchasing of goods, through both the clear web and the dark web. Unlike the clear web (also called the "surface web"), which refers to information available to the public and indexed by commonly available search engines, the dark web (or darknet/darknets, the terms are used interchangeably below) is made up of darknets of encrypted networks, allowing both the site owner and the users to remain relatively anonymous and untraceable.[23]

[16] Garrick Hileman and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge, United Kingdom of Great Britain and Northern Ireland, Cambridge Centre for Alternative Finance, 2017).

[17] Desmond and others, "Evaluating cryptocurrency laundering as a complex socio-technical system".

[18] Angela S. M. Irwin and Caitlin Dawson, "Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help", *Journal of Money Laundering Control*, vol. 22, No. 1 (January 2019), pp. 110–131.

[19] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: the FATF Recommendations* (Paris, 2012).

[20] Irwin and Turner, "Illicit Bitcoin transactions"; Goodell and Aste, "Can cryptocurrencies preserve privacy and comply with regulations?".

[21] Sesha Kethineni, Yin Cao and Cassandra Dodge, "Use of Bitcoin in darknet markets: examining facilitative factors on Bitcoin-related crimes", *American Journal of Criminal Justice*, vol. 43, No. 2 (June 2018), pp. 141–157.

[22] United Nations Office on Drugs and Crime (UNODC), "UNODC launches training to tackle cryptocurrency-enabled organized crime", 8 May 2017.

[23] Darren Guccione, "What is the dark web? How to access it and what you'll find", *The State of Cybersecurity*, 4 July 2019.

15. Darknet marketplaces (also described as "cryptomarkets")[24] provide buyers and sellers anonymity, and on such marketplaces principally cryptocurrencies are used for payment to facilitate the selling and trading of goods such as weapons and illicit drugs.

16. According to the European Union Agency for Law Enforcement Cooperation (Europol), compromised personal, medical and financial data are a key commodity on darknet markets and play a crucial role in activities such as frauds, phishing, identity theft and the takeover of accounts. However, while darknet marketplaces offer a range of counterfeit and pirated goods for sale, most illicit trade still occurs on the surface web.[25] Match-fixing and gambling have been increasingly used on the dark web in support of money-laundering routes, especially by transnational organized criminal groups.[26] The European Regional Preparatory Meeting for the Fourteenth Congress also stressed the need to address the use of the darknet for the commission of hate crimes.[27]

17. In the area of drugs, the *World Drug Report 2019* stated that purchases of drugs on the darknet were increasing in the long term, although they may have declined from 2018 to 2019. Data from the Global Drug Survey 2019 suggested that the purchase of drugs through the darknet was still a very recent phenomenon, with 48 per cent of people who reported purchasing drugs through the darknet in 2019 having started to use the darknet for such purposes in the previous two years and a further 29 per cent in the two preceding years.[28]

18. Darknet drug markets may have the potential to kickstart changes in the patterns and prevalence of drug use[29] as they can reduce certain risks for buyers and sellers, such as violent encounters in neighbourhoods where drug sales occur,[30] coercion and arrest.[31] However, Internet-facilitated drug sales bring their own risks. The biggest risks are likely to occur during the related "offline" activities.[32] Internet-facilitated drug sales may also be related to increases in overdoses to the extent that they increase the ease of experimentation and the availability of higher potency drugs.[33]

19. There have been notable successes in dismantling large darknet markets. According to Europol, however, criminals are exploring alternative means of circumventing law enforcement actions. A new trend is the emergence of business models in which criminals use multiple identities, through the use of multiple profiles on different online platforms, which, in turn, facilitates operations by various individuals rather than a single person.[34]

[24] Julian Broseus and others, "Studying illicit drug trafficking on Darknet markets: structure and organization from a Canadian perspective", *Forensic Science International*, vol. 264, 5 March 2016, p. 7.

[25] European Union Agency for Law Enforcement Cooperation (Europol), European Cybercrime Centre, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (The Hague, 2018), p. 49.

[26] Robin Cartwright and France Cleland Bones, *Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions* (Geneva, Global Initiative against Transnational Organized Crime, 2017), p. 29.

[27] See A/CONF.234/RPM.5/1, para. 36 (g).

[28] *World Drug Report 2019: Global Overview of Drug Demand and Supply* (United Nations publication, Sales No. E.19.XI.8 (Booklet 2)).

[29] Judith Aldridge and David Décary-Hétu, "Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets", *International Journal of Drug Policy*, vol. 35, September 2016, p. 12.

[30] Julia Buxton and Tim Bingham, *The Rise and Challenge of Dark Net Drug Markets*, Policy brief, No. 7 (Swansea, United Kingdom, Global Drug Policy Observatory, January 2015), pp. 1–24.

[31] Buxton and Bingham, *The Rise and Challenge of Dark Net Drug Markets*. See also David Décary-Hétu, Masarah Paquet-Clouston and Judith Aldridge, "Going international? Risk taking by cryptomarket drug vendors", *International Journal of Drug Policy*, vol. 35, September 2016, p. 71.

[32] Judith Aldridge and Rebecca Askew, "Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement", *International Journal of Drug Policy*, vol. 41, March 2017, pp. 101–109.

[33] Nathaniel Popper, "Opioid dealers embrace the dark web to send deadly drugs by mail", *New York Times*, 10 June 2017.

[34] Europol, European Cybercrime Centre, *Internet Organised Crime Threat Assessment (IOCTA) 2019* (The Hague, 2019), p. 45.

20. There are a number of challenges in conducting investigations on the dark web. A major problem is that information in the darknet is unindexed, and as a result investigators cannot easily locate that information using search engines or keywords. Furthermore, criminals make use of decentralized platforms for hosting their web servers, thus enabling a proliferation of services that may be more difficult to detect.[35]

21. On the other hand, there are opportunities for law enforcement authorities to monitor darknet markets and carry out online investigations.[36] In this context, an array of tools may provide solutions, including web crawlers that can be employed to automate the indexing of online data on a recurring basis, data mining tools for the search of huge datasets, cryptocurrency analytical tools to trace the path of payments, and blockchain software used for tracking evidence.[37] Technical assistance is important and UNODC has been active in training activities focusing on investigative techniques for the dark web.

C. Firearms: technology-related security threats

1. Techno-polymers in firearms manufacturing

22. Industrial polymers are bound to assume an increasingly dominant role in the arms industry, posing challenges for the effective implementation of the provisions on tracing and record-keeping of firearms contained in 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. This appearance of industrial polymers jeopardizes the ability of competent authorities to adequately detect, investigate and prosecute related offences.

23. The Modular Small-arms-control Implementation Compendium (MOSAIC) – a collection of non-binding good practices on small arms control that builds on the acquis of relevant international instruments: the Firearms Protocol, the Programme of Action on Small Arms and the related International Tracing Instrument and the Arms Trade Treaty – can assist countries in addressing the challenges posed by polymer frames and receivers.

2. Modular weapons

24. New technologies and existing legislative loopholes have resulted in both licit and illicit markets being flooded with modification, conversion and manufacturing kits that enable gun owners, with minimal technical knowledge, to transform their firearms or even produce completely functional ones.

25. The Firearms Protocol applies to "parts and components", but its marking requirements (article 8) apply only to "firearms". This can be particularly problematic in relation to modular weapons.[38] Addressing this challenge may require measures such as the identification of a control component for all firearms, whether standard or modular, for marking, record-keeping and tracing purposes; the determination of what information should be marked on the control component to avoid duplication of serial numbers; and the provision of guidance on unique identification for tracing purposes, in particular for modular weapons.[39]

[35] International Criminal Police Organization (INTERPOL) "Innovation report: anonymous networks and darknet" (September 2018), pp. 12–13.

[36] European Monitoring Centre for Drugs and Drug Addiction and Europol, *Drugs and the Darknet: Perspectives for Enforcement, Research and Policy* (Luxembourg, 2017), p. 60 ff.

[37] INTERPOL, "Innovation report", p. 14. See also Shira Stein, "Law enforcement adapts to using cryptocurrency to catch criminals", *Securities Regulation and Law Report*, 49 SRLR 1029 (Arlington, Virginia, Bureau of National Affairs, 2017).

[38] Giacomo Persi Paoli, "From firearms to weapon systems: challenges and implications of modular design for marking, record-keeping, and tracing", in *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, No. 32, Benjamin King and Glenn McDonald, eds. (Geneva, Small Arms Survey, 2015), p. 23.

[39] Ibid., p. 40.

3. Additive manufacturing (3D printing)

26. Additive manufacturing – colloquially known as three-dimensional printing, or 3D printing – is an emerging technology with potential local, national and international security implications in the near and long terms. The development and spread of additive manufacturing could significantly accelerate weapon proliferation and may have dramatic consequences for everyday crime. Moreover, 3D-printed firearms may have a negative impact on the efficacy of firearms registration and licensing schemes and ballistic databases used for police investigations.

27. Article 3 (d) and article 5, paragraph 1 (a), of the Firearms Protocol, on the illicit manufacturing of firearms, would apply to firearms produced using 3D printing in the same way as they apply to traditionally manufactured firearms. However, the downloading of digital files for the 3D printing of firearms seems to fall outside the scope of the Protocol, a situation that calls for urgent legislative responses.

28. Many existing laws and offences regarding the unlicensed manufacture, creation and possession of firearms cover 3D-printed firearms, although not necessarily the possession or distribution of design files.[40] Laws addressing the illicit manufacture of firearms may need to determine the culpability of third parties in cases where machinery is made available to people who may wish to produce firearms using additive manufacturing techniques.[41]

29. A comprehensive regulatory approach would have to include domestic and international actors, as well as both public and private sectors. The dual-use potential of additive manufacturing makes it impossible to limit the spread of this technology without also curtailing its many benefits.[42] As with any emerging technology, it will be important to provide for the training and education of law enforcement personnel.

4. Trafficking in firearms on the dark web

30. The dark web has the potential to become a platform of choice for organized criminal groups and individuals who want to purchase firearms anonymously or for illegal purposes.[43] In response to a study submitted by the United Nations Office for Disarmament Affairs to the First Committee of the General Assembly in 2018, prepared on the basis of a larger research project conducted by RAND Europe in 2017,[44] it was observed that there was a dire need for new international cooperation to combat illicit arms sales made possible by the anonymity of the dark web.[45]

31. The proportion of arms sales that take place on the dark web appears to be smaller than that for other illicit items.[46] A recent study focusing on only weapons-related listings on the dark web found that firearms listings were the most common, making up 42 per cent of all listings on the dark web, followed by arms-related digital products at 27 per cent, and other products such as ammunition at 22 per cent.[47]

[40] INTERPOL Innovation Paper, "3D and 4D printing", INTERPOL Global Complex for Innovation, 2018, p. 6.

[41] N. R. Jenzen-Jones, "Small arms and additive manufacturing: An assessment of 3D-printed firearms, components, and accessories", in *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, No. 32, Benjamin King and Glenn McDonald, eds. (Geneva, Small Arms Survey, 2015), pp. 63–64.

[42] Trevor Johnston, Troy D. Smith and J. Luke Irwin, "Additive manufacturing in 2040: powerful enabler, disruptive threat", document No. PE-283-RC (Santa Monica, California, RAND Corporation, 2018), p. 17.

[43] RAND Europe, "International arms trade on the dark web" (2019), Findings section, para. 8.

[44] Giacomo Persi Paoli and others, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, California, RAND Corporation, 2017).

[45] Giacomo Persi Paoli, *The Trade in Small Arms and Light Weapons on the Dark Web*, United Nations Office for Disarmament Affairs (UNODA) Occasional Papers, No. 32 (United Nations publications, Sales No. E.19.XI.1), p. ix.

[46] Damien Rhumorbarbe and others,"Characterising the online weapons trafficking on cryptomarkets", *Forensic Science International*, vol. 283, December 2018, pp. 16–20.

[47] RAND Europe, "International arms trade on the dark web" (2019), Findings section, para. 4.

32. Understanding the size and the scope of the illicit arms trade on the dark web is essential to gain a better understanding of the severity of the threat and the implications for law enforcement authorities. At the national level, policymakers need to ensure that law enforcement authorities are appropriately staffed, trained and equipped to address related challenges. Existing international legal frameworks, in particular the Organized Crime Convention and its Firearms Protocol, may provide the basis for comprehensive approaches for tackling the phenomenon. An in-depth analysis of whether existing brokering regulations, provided by the Firearms Protocol (article 15) and the Arms Trade Treaty (article 10), would be applicable, is required.[48]

5. Lethal autonomous weapons

33. Although there is no official recognition of the existence of fully autonomous weapons, the idea of using artificial intelligence to control such weapons has fuelled strong debates. In 2016, the Fifth Review Conference of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects established the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. In its 2019 session, the Group recommended that the High Contracting Parties endorse the guiding principles affirmed by the Group.[49]

D. Trafficking in persons

34. Research over past years and direct evidence show that technology is being used by human traffickers during all stages of the crime, including recruitment, control and exploitation of victims.

35. One reason that technology is harnessed by traffickers is that it enables them to operate anonymously and hide their identity. Additionally, cryptocurrency allows traffickers to conduct financial transactions and move criminal proceeds anonymously. Another reason is that technology facilitates the recruitment and exploitation of victims by traffickers. Online classified advertising and social networking sites can be used as "conduits for human trafficking".[50]

36. Further, the misuse of technology can make it easier for traffickers to engage in transactions with users, enter new marketplaces and expand criminal operations. Traffickers can use live-streaming to reach a broader market of customers who may never have physical contact with the victim.[51]

37. Moreover, the misuse of technologies can help traffickers control and coerce victims. Traffickers may take advantage of location tracking to facilitate the exploitation of victims. Even after victims have escaped the traffickers' grasp, they can still be tracked as the abusers discover their whereabouts using location trackers on the victims' mobile phones.

38. At the same time, law enforcement authorities already use location tracking to detect the position of suspected traffickers or other individuals participating in the trafficking network. Making use of the location tracking data of the victims is the

[48] Simonetta Grassi and Mareike Buettner, "Annex: overview of international legal instruments and their applicability to illicit firearms trafficking on the dark web", in Paoli and others, *Behind the Curtain*, p. 101.

[49] CCW/GGE.1/2019/3, annex IV.

[50] Mark Latonero, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, Centre on Communication Leadership and Policy Research Series (Los Angeles, University of Southern California, September 2011), p. 8.

[51] Inter-Agency Coordination Group against Trafficking in Persons, "Human trafficking and technology: trends, challenges and opportunities", Issue brief, No. 7 (2019), pp. 1–2.

other side of the same coin, given that victims can be treated as "walking databases of evidence".[52]

39. The use of technological interventions in anti-trafficking efforts requires collaboration across sectors. The information and communication technologies industry and international organizations have partnered to explore how technologies can be harnessed to prevent trafficking in persons and support the rehabilitation of victims. Tech Against Trafficking, a coalition of leading technology companies, academic institutions and the International Organization for Migration, provides a list of technological solutions utilized for countering human trafficking.[53]

40. Capacity-building for all actors involved is pivotal to address the challenges posed by the use of technology for trafficking in persons. Careful thought must be given to the development, use, maintenance, monitoring and evaluation of technology used by practitioners to combat trafficking in persons.[54] However, the developers of relevant tools need to anticipate and accommodate the differences that exist among users at risk of being trafficked.[55]

E. Smuggling of migrants

41. Information and communication technologies have become an important tool widely used by migrants and recruiters alike to transmit information about routes, services and prices.[56] Further, social media has increased the capacity of smugglers to change routes in reaction to the responses of law enforcement authorities in transit countries, thereby increasing the effectiveness of smuggling operations and hindering the investigation and prosecution of such crimes.[57]

42. The rapid development of mobile technology can have implications for the relationship between migrants and smugglers. In several Facebook groups, migrants can check the reliability of certain smugglers and share information on who is best to contact. That has been described as a "hierarchy in trustworthiness".[58]

43. Technologies could also be used for financial payment, as payments to smugglers are primarily made through online payment systems. Cryptocurrencies may increase the ease with which smugglers are able to receive, hide and move money. Such currencies can aid money-laundering and help smugglers avoid investigation and apprehension by providing anonymity and reducing the need to carry large quantities of cash.

44. Technology further plays a major role in making available fraudulent travel or identity documents that facilitate the smuggling of migrants. Various types of equipment are used to fraudulently create, alter or copy passports. In some cases,

[52] Felicity Gerry, Julia Muraszkiewicz and Niovi Vavoula, "The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns", *Computer Law and Security Review*, vol. 32, No. 2 (April 2016), pp. 210–211.

[53] Business for Social Responsibility, "List of technology tools and initiatives identified by tech against trafficking", 15 January 2019.

[54] Inter-Agency Coordination Group against Trafficking in Persons, "Human trafficking and technology", p. 4.

[55] See Mark Latonero, Bronwyn Wex and Meredith Dank, *Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study* (Los Angeles, University of Southern California, Annenberg Center on Communication Leadership and Policy, 2015), p. 11.

[56] Europol and INTERPOL, "Migrant smuggling networks: executive summary" (May 2016), p. 8.

[57] CTOC/COP/WG.7/2018/2, para. 25.

[58] Judith Zijlstra and Ilse van Liempt, "Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys", *International Journal of Migration and Border Studies*, vol. 3, Nos. 2 and 3 (March 2017), pp. 176–177.

technologically advanced tools have been used to create high-quality forgeries ("mirror-grade" passports).[59]

45. However, technological innovations can be considered from multiple angles and not only from the perspective of the benefits for smugglers. Digitalization also reduces the information gaps on which smugglers can thrive. The Internet can be leveraged to assist migrants to connect with social networks of support and information. A recent trend that has emerged from a technology-driven shift is that an increasing number of migrants are self-sufficient throughout the migration process and less dependent on smugglers. That gives migrants greater autonomy and reduces their vulnerability to exploitation.[60]

46. How migrants use social media differs according to their nationality, ethnicity, region of origin and educational background, as well as depending on their access to the Internet.[61] Evidence has shown that there is a digital divide among migrant groups, which is based on inequalities in physical access to, and use of, digital technology, the skills necessary to use the different technologies effectively and the ability to pay for the services.[62]

47. From a law enforcement perspective, there is growing interest in finding ways to exploit technology to disrupt networks for the smuggling of migrants. Further, the use of evidence obtained from social media and/or through the use of technology may support the testimonies of smuggled migrants in related criminal proceedings.

48. The appropriate use of technology assists governments, the private sector and non-governmental organizations in preventing and mitigating smuggling of migrants within their respective areas of competence. It is therefore vital to increase the effectiveness of criminal justice responses and establish incentives and partnerships with online service providers to improve the monitoring, detection and reporting of smuggling-related content.

F. Online abuse and exploitation of children

49. Although child sexual abuse and exploitation existed before the advent of the Internet, the online dimension of these crimes has enabled offenders to interact with each other and obtain child sexual exploitation material online. Further, the growing number of younger children with access to the Internet has given offenders an opportunity to reach children more easily – compared with the offline environment – and that, in turn, has had considerable implications for the modus operandi of related crimes.

50. Advances in technology have become instrumental in the commercial sexual exploitation of children. Child sex tourists can make use of cloud computing to store images or videos, thus avoiding the risks associated with physically transporting child sexual exploitation material. Moreover, mobile telephone technology connects organizers, victims and consumers of child sexual exploitation and abuse, thus reducing the need for producers and distributors to be physically present at transactions, which, in turn, serves to better insulate them from detection.

[59] UNODC Regional Office for South-East Asia and the Pacific, *Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption* (Bangkok, 2019), p. 26.

[60] UNODC, Doha Declaration, Tertiary, Education for Justice University Module Series, Trafficking in Persons and Smuggling of Migrants, "Module 14: links between cybercrime, trafficking in persons and smuggling of migrants–technology in smuggling of migrants". Available at www.unodc.org/e4j/.

[61] European Commission, "The use of social media in the fight against migrant smuggling", European Migration Network (EMN) Inform (September 2016).

[62] Alam Khorshed and Sophia Imran, "The digital divide and social inclusion among refugee migrants: a case in regional Australia", *Information Technology and People*, vol. 28, No. 2 (June 2015), pp. 344 ff.

51. The main forms of child abuse and exploitation facilitated by information and communication technologies include exposure to pornography, online grooming and unwanted sexual solicitations online, and many such acts of exploitation feature inappropriate sexual activities with children. A relevant UNODC study draws attention to new forms of child abuse and exploitation such as user-generated content, self-generated content including sexting, broadcasting of live sex abuse and "made-to order" child sexual abuse material.[63]

52. According to Europol, the broadcasting of live sex abuse has become an established threat, and it takes place through social media applications, video chat applications, gaming platforms and online chat rooms. Furthermore, there appears to be a move from computer usage to smartphones and tablets and from cable Internet to Wi-Fi and mobile Internet.[64]

53. One of the most important threats in the online distribution of child sexual exploitation material is the continuous increase in the use of the darknet. According to the Internet Watch Foundation, disguised websites using the "digital pathway" method to hide child sexual abuse imagery continue to be a significant problem. Moreover, the Foundation saw a steady increase of child sexual abuse web addresses in recent years: from 68,092 in 2015 to 105,047 in 2018.[65]

54. Further, as online child sexual offenders become more technically sophisticated, they will continue to seek new ways to avoid detection. Recently, there has been a shift from large forums to the formation of small user groups facilitated by mobile messaging applications with end-to-end encryption.

55. The absence in a number of countries of applicable legal provisions for regulating emerging forms of child abuse and the differences in the laws that protect children and define the age of consent pose significant problems and decrease the probability of successful detection, investigation and prosecution.

56. Technology may also offer ways for law enforcement authorities to combat related problems.[66] Innovations in methods and techniques such as data mining and analytics improve forensic processes to advance investigations. Techniques using information technology should be applied while respecting the boundaries of protecting human rights due to the traumatic nature of child sexual exploitation and the age and vulnerability of child witnesses.

57. Databases have also been created for the purpose of uploading child sexual abuse material for investigative purposes, such as the International Child Sexual Exploitation database of the International Criminal Police Organization. In the United States of America, the database of the National Center for Missing and Exploited Children serves as a central repository for child sexual abuse material.[67]

58. Efforts to effectively combat child abuse and exploitation facilitated by information and communication technology requires a multi-stakeholder approach, including and actively involving children, families, communities, governments, civil society and the private sector.[68]

[63] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna, 2015), pp. 21 ff.

[64] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, p. 35.

[65] Internet Watch Foundation, *Once Upon a Year* (Cambridge, United Kingdom, 2018), pp. 19 and 43.

[66] Victoria Brains, "Online child sexual exploitation: towards an optimal international response", *SSRN Electronic Journal*, 29 August 2018.

[67] UNODC, Doha Declaration, Tertiary, Education for Justice University Module Series, Cybercrime, "Module 12: interpersonal cybercrime–online child sexual exploitation and abuse". Available at www.unodc.org/e4j/.

[68] UNODC, *Study on the Effects of New Information Technologies*.

G. Artificial intelligence and robotics

59. After the Internet and mobile technology triggered the “third industrial revolution”, artificial intelligence technologies, driven by big data,[69] are fuelling a “fourth industrial revolution”. While this can be beneficial for global development and societal change, contributing to the achievement of the Sustainable Development Goals, legal, ethical and societal concerns and challenges also arise. In the field of law enforcement, advancements in artificial intelligence can bring both opportunities and risks, and thus a strategic approach and investments in efforts and resources are required.[70]

60. Almost all regional preparatory meetings for the Fourteenth Congress stressed the necessity and significance of exploring ways and means to enable criminal justice and law enforcement practitioners to utilize and take full advantage of evolving technologies such as artificial intelligence and information and communication technologies, including big data, in the fight against crime.[71]

61. There are relevant discussions related to, inter alia, the use of artificial intelligence for conducting virtual autopsies, crime prediction systems to support police to optimize resources, behaviour detection tools, blockchain-based traceability approaches that respect privacy, and autonomous patrol vehicles.[72] Moreover, encouraged by advancements in artificial intelligence which make robotics “smarter” and capable of replacing human beings in many functions and tasks, an increasing number of law enforcement authorities adopt such technological advances in a variety of their operations. The level of utilization of robotics is far from homogenous, as some countries are more advanced than others in research and use of such technologies.[73]

62. Artificial intelligence and machine learning seem to provide an increasingly efficient shield against money-laundering. Like the algorithms that help online retailers target customers, artificial intelligence and machine learning can support more insightful and accurate due diligence policies by interpreting the signals that indicate criminal activity and analysing vastly greater quantities of data, and do it more reliably. Moreover, machine learning has been increasingly deployed by social media platforms to block illicit content and fake news. Businesses have been using artificial intelligence for higher risk management and responsive fraud detection for the prevention and prediction of crimes.

63. However, artificial intelligence is very much a double-edged sword, as it can lead to great changes in the way that law enforcement authorities approach the task of policing, but it also enhances the modi operandi of criminal and terrorist groups and can even facilitate the emergence of new forms of crime.[74] In what can eloquently be described as a fight for the “survival of the fittest”,[75] the priority can be

[69] Victor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live Work and Think* (London, John Murray, 2013).

[70] The United Nations Interregional Crime and Justice Research Institute (UNICRI) has established a Centre for Artificial Intelligence and Robotics in The Hague, to serve as an international resource on matters related to artificial intelligence and robotics.

[71] A/CONF.234/RPM.1/1, para. 61 (j); A/CONF.234/RPM.2/1, para. 79 (k); A/CONF.234/RPM.3/1, para. 56 (f); and A/CONF.234/RPM.4/1, para. 57 (e).

[72] INTERPOL and UNICRI, “Artificial intelligence and robotics for law enforcement” (Turin, Italy, 2019), p. v.

[73] Ibid., p. 6.

[74] A 2018 report examined the criminal misuse of artificial intelligence and identified three main categories of related threats: (a) those associated with digital security; (b) those linked to physical security; and (c) those pertaining to political security (proliferation of fake news and automated disinformation or influence campaigns to affect voting behaviour and possibly undermine the ability to sustain truthful public debate). See Miles Brundage and others, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (February 2018).

[75] INTERPOL Innovation Paper, “Artificial intelligence”, INTERPOL Global Complex for Innovation, 2018, p. 2.

summarized thus: foster artificial intelligence-led policing to combat artificial intelligence-led crimes.

H. International cooperation in criminal matters and the use of technology

64. An ongoing debate in the field of international cooperation in criminal matters is how central authorities can fully benefit from the use of modern technology. From a policy perspective, in 2016 the Conference of the Parties to the United Nations Convention against Transnational Organized Crime encouraged States parties to make the fullest and most effective use of available technology to facilitate cooperation between central authorities.[76]

65. The increasing need for enhanced international cooperation is subject to the availability of resources, including "technology resources", such as networks for securely transmitting information, equipment facilitating communication (e.g., teleconferences and videoconferences) and case management systems to track incoming and outgoing requests. The increasing need for resources may also be linked to more efficiency in handling mutual legal assistance requests involving electronic evidence (through, for example, the establishment of specialized units within the central authorities).

66. 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.[77]

67. In terms of transmission of mutual legal assistance requests, the Latin American and Caribbean Regional Preparatory Meeting for the Fourteenth Congress discussed the use of electronic means for this purpose, which was highlighted as a good practice in certain countries in the region.[78] The Preparatory Meeting recommended the promotion of the use of technology to make international cooperation in criminal matters more efficient, taking into consideration, inter alia, agreements between central authorities for the electronic transmission of international cooperation requests in accordance with national legislation.[79]

68. UNODC has undertaken action to promote international cooperation, including through tailor-made tools and technological innovations: the knowledge management portal known as Sharing Electronic Resources and Laws on Crime (SHERLOC), the directory of competent national authorities and the redeveloped version of the Mutual Legal Assistance Request Writer Tool.[80]

69. UNODC has been actively supporting intergovernmental processes in which international cooperation involving electronic evidence has emerged as a policy and legal priority. Examples of such processes include the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime,[81] the thematic discussion on cybercrime at the twenty-seventh session of the Commission on Crime Prevention and Criminal Justice, held in May 2018,[82] and pertinent work of

[76] Conference resolution 8/1.

[77] Asian Development Bank and Organization for Economic Cooperation and Development, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (2017), p. 31.

[78] A/CONF.234/RPM.3/1, para. 72.

[79] Ibid., para. 79 (n).

[80] Available at www.unodc.org/mla/en/index.html.

[81] UNODC, Cybercrime, "Meeting of the IED on cybercrime". Available at www.unodc.org.

[82] See the guide for that thematic discussion (E/CN.15/2018/6).

the Working Group on International Cooperation of the Conference of the Parties to the Organized Crime Convention.

I. Ethical considerations: procedural and human rights safeguards

70. 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.

71. Facial recognition software, for example, is being used by law enforcement professionals to much more rapidly identify suspects. However, critics worry it can lead to abusive government surveillance, corporate manipulation and the end of privacy. Furthermore, the data retention aspect of biometric systems may jeopardize privacy through potential data misuse.[83]

72. Another example is that of predictive policing or analytics. In the past years, 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. However, the risk is that the use of predictive policing for profiling may result in stigmatizing individuals and groups and, thus, forms of discrimination based on algorithms.[84]

73. In the area of trafficking in persons and in exploring the interplay of the use of technology with human rights and data protection,[85] it is vital to ensure the enhanced protection of victims. Counter-trafficking solutions should be designed with careful oversight so that they do not overstep rights to privacy or unduly target certain groups,[86] while ensuring that victims also have safe access to technology.[87]

74. Another important factor is the compliance with procedural safeguards for the admissibility in court of evidence obtained from special investigative techniques, including those involving the use of technology. The conduct of special investigative techniques is subject to relevant provisions of domestic laws and applicable multilateral instruments.[88] In most jurisdictions, the gathering of evidence requires strict adherence to safeguards against potential abuses of authority, including judicial or independent oversight of the use of these techniques and observance of the principles of legality, subsidiarity and proportionality.[89] Electronic evidence must comply with established procedures in order to be admissible.[90] The application of general principles of domestic procedural laws and national jurisprudence on the

[83] Max Snijder, *Biometrics, Surveillance and Privacy* (Ispra, Italy, European Reference Network for Critical Infrastructure Protection (ERNCIP) Thematic Group Applied Biometrics for the Security of Critical Infrastructure, 2016), pp. 4 ff.

[84] See Eva Schlehahn and others, "Benefits and pitfalls of predictive policing", in *2015 European Intelligence and Security Informatics Conference: EISIC 2015*, Joel Brynielsson and Moi Hoon Yap, eds. (Piscataway, New Jersey, Institute of Electrical and Electronics Engineers, Inc, 2015), pp. 145–148; Albert Meijer and Martijn Wessels, "Predictive policing: review of benefits and drawbacks", *International Journal of Public Administration*, vol. 42, No. 12 (February 2019).

[85] See Inter-Agency Coordination Group Against Trafficking in Persons, "Human trafficking and technology", p. 5.

[86] Mark Latonero and others, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Research Series on Technology and Human Trafficking (November 2012), p. 38.

[87] Gerry, Muraszkiewicz and Vavoula, "The role of technology in the fight against human trafficking", p. 211.

[88] See article 20 of the United Nations Convention against Transnational Organized Crime and article 50 of the United Nations Convention against Corruption.

[89] For the relevant jurisprudence of the European Court of Human Rights, see Dimosthenis Chrysikos, "Article 50: special investigative techniques", in *The United Nations Convention against Corruption. A Commentary*, Cecily Rose, Michael Kubiciel and Oliver Landwehr, eds., Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2019), pp. 507 ff.

[90] E/CN.15/2018/6, para. 30.

admissibility of evidence obtained in forensic cryptocurrency investigations is a new and challenging area requiring further consideration and the sharing of experiences.[91]

75. As the use of artificial intelligence and robotics by law enforcement becomes more pervasive, it becomes increasingly important to ensure that such use is ethical. Initiatives of a "soft law" nature have been undertaken to minimize the risks of violation of fundamental rights stemming from the use of artificial intelligence systems by law enforcement authorities and to ameliorate the ambiguity of legal liability surrounding the ethical use of artificial intelligence and robotics in general.[92]

76. A fundamental question, however, is whether society in general is ready and well prepared to accept practices such as the establishment of an extensive network of surveillance devices, even if it is in the interests of public safety and security.[93] Decisions concerning technology should be underpinned by a broad social dialogue on its costs, benefits and the norms applicable. The issue of persuading the public of the benefits of technology in the law enforcement and criminal justice areas is part of a general debate that needs to take place consistently in order to ensure that the competent authorities do not lose the confidence of the communities and citizens that they are mandated to protect. This debate should also echo the "other side of the coin": the criticism that increased reliance on technology may potentially also lead to an increased reliance on both coercive surveillance and control strategies.[94]

77. The High-Level Panel on Digital Cooperation recommended that the Secretary-General institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age, in a proactive and transparent process.[95]

78. 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. To avoid the use of technologies as a "Trojan horse" for potential infringements of fundamental rights, technology development needs to be continuously monitored and its impact evaluated.

III. Conclusions and recommendations

79. Inspired by Greek mythology, one could formulate the issue thus: is technology, ultimately, a panacea (a remedy claimed to cure all diseases, named after the daughter of Asclepius) for crime prevention? Or is it a Pandora's box, a process that turns out to have serious effects in terms of expanding opportunities for crime (similar to the myth of Pandora opening the jar and allowing all evils to flow out)?

80. The truth lies in the middle, away from Manichean answers. Technology is inevitably a mixed blessing. Law enforcement and criminal justice authorities benefit from advancements of technology. At the same time, the explosion of technological innovations provides fertile ground for crime to flourish. The "crime landscape" has

[91] Michael Fröwis and others, "Safeguarding the evidential value of forensic cryptocurrency investigations" (2019).

[92] The Institute of Electrical and Electronics Engineers (IEEE) issued a global treatise regarding the ethics of autonomous and intelligent systems (ethically aligned design) to align technologies to moral values and ethical principles. See IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Pascataway, New Jersey, 2019).

[93] INTERPOL and UNICRI, "Artificial intelligence and robotics for law enforcement", p. 14.

[94] James Byrne and Gary Marx, "Technological innovations in crime prevention and policing: a review of the research on implementation and impact", *Cahiers Politiestudies*, vol. 20, No. 3 (2011), p. 30.

[95] United Nations, *The Age of Digital Interdependence: Report of the Secretary-General's High-level Panel on Digital Cooperation* (June 2019), recommendation 3A.

been changing drastically due to various applications of modern technology, and competent authorities need to catch up.

81. The outcome of the ongoing *bras de fer* between criminals and defenders of the rule of law will largely depend on whether investments are made in training and crime prevention and criminal justice strategies are continuously adapted to address emerging challenges while taking into account ethical and human rights considerations.

82. The Fourteenth United Nations Congress on Crime Prevention and Criminal Justice may wish to consider the following recommendations:

(a) Member States should identify and address gaps in their legal systems to ensure the effective investigation and prosecution of technology-facilitated crimes, including by adopting new laws and/or updating existing ones with technologically neutral wording, and enhancing international cooperation;

(b) Member States should foster and expand partnerships and synergies with various stakeholders, including international and regional organizations, civil society, the private sector and academia, to enhance research, innovation, development and the use of technology in the fields of law enforcement and criminal justice;

(c) Member States should identify and assess money-laundering and terrorist financing risks emerging from activities or operations involving virtual assets service providers; apply a risk-based approach to ensure that measures to prevent or mitigate money-laundering and terrorist financing are commensurate with the risks identified; and require virtual assets service providers to identify, assess and take effective action to mitigate money-laundering and terrorist financing risks;

(d) Member States should increasingly invest in appropriate training to improve capacities to effectively tackle issues raised by cryptocurrencies during investigations;

(e) Member States should include in their legislation provisions relevant to the possession, publication and transfer of digital materials that can be used for the eventual manufacture of firearms, and pursue capacity-building activities to increase skills to prevent, detect, investigate and prosecute those acts as well as trafficking in firearms on the darknet;

(f) UNODC should continue to promote regular meetings of communities of practitioners to ensure that investigators are up-to-date with the new modi operandi for firearms manufacture and transfer and with the corresponding investigative techniques;

(g) Member States should devote particular attention to building the expertise and capacity of competent authorities in all relevant sectors to allow for the optimal use of technology against trafficking in persons, while protecting the rights of victims;

(h) UNODC should further develop its technical guidance and support to Member States to more effectively identify and implement technology-based criminal justice system measures to prevent, investigate and prosecute trafficking in persons and smuggling of migrants;

(i) Member States should take legislative or other measures to facilitate the detection, by Internet service and access providers and other relevant entities, of child sexual exploitation and sexual abuse materials and to ensure the reporting and removal of such materials;

(j) Member States should implement policies and share best practices, including on support programmes for victims and the mainstreaming of a gender perspective, in order to protect children from sexual exploitation and abuse;

(k) Member States should advance understanding of the risks posed by the malicious use of artificial intelligence and continuously monitor developments in new technologies to ensure preparedness, accountability, transparency and integrity;

promote ethical standards in using those technologies; and secure the confidence and trust of citizens and communities in such use;

(l) Member States, in cooperation with UNODC and other international organizations, should promote technical assistance and training to enhance the skills of practitioners and central authorities on the use of technology to expedite international cooperation.