



Fourteenth United Nations Congress on Crime Prevention and Criminal Justice

Distr.: Limited
11 March 2021

Original: English

Kyoto, Japan, 7–12 March 2021

Agenda item 6

**International cooperation and technical assistance
to prevent and address all forms of crime**

Report of Committee II: workshop 4

Addendum

Current crime trends, recent developments and emerging solutions, in particular new technologies as means for and tools against crime

Proceedings

1. At its 4th to 6th meetings, on 10 and 11 March 2021, Committee II held the workshop on current crime trends, recent developments and emerging solutions, in particular new technologies as means for and tools against crime. The Korean Institute of Criminology and the National Institute of Justice of the United States Department of Justice, both of them members of the United Nations crime prevention and criminal justice programme network, assisted in the preparation and organization of the workshop. The Committee had before it the following documents:

- (a) Background paper prepared by the Secretariat on the workshop on current crime trends, recent developments and emerging solutions, in particular new technologies as means for and tools against crime ([A/CONF.234/11](#));
- (b) Working paper prepared by the Secretariat on developments regarding crime prevention and criminal justice as a result of the coronavirus disease (COVID-19) pandemic ([A/CONF.234/15](#));
- (c) Discussion guide for the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice ([A/CONF.234/PM.1](#));
- (d) Reports of the regional preparatory meetings for the Fourteenth Congress ([A/CONF.234/RPM.1/1](#), [A/CONF.234/RPM.2/1](#), [A/CONF.234/RPM.3/1](#), [A/CONF.234/RPM.4/1](#) and [A/CONF.234/RPM.5/1](#)).

2. The three sessions of the workshop were moderated respectively by the following experts: Phelan Wyrick, Director, Research and Evaluation Division, National Institute of Justice; Han-Kyun Kim, Senior Research Fellow, Korean Institute of Criminology; and Dimosthenis Chrysikos, Crime Prevention and Criminal Justice Officer, United Nations Office on Drugs and Crime.

3. At the 4th meeting, on 10 March, the Chair of Committee II made an introductory statement. The moderator of the first session then briefly introduced the sub-topics of the session. The following panellists discussed cryptocurrencies and darknet markets, as well as technology-related issues in the field of firearms: Anthony

Teelucksingh (United States of America) as keynote speaker; Hayato Shigekawa (Chainanalysis/private sector); Thomas Holt (Michigan State University (U.S.A.)); José Romero Morgaz (European Commission); Anna Alvazzi del Frate (Alliance of NGOs on Crime Prevention and Criminal Justice); and Maria Jiménez Victorio (Spain, speaking as individual expert).

4. Statements were made by the representatives of China, France, Indonesia, Mexico, Morocco, Russian Federation and United States of America.

5. At the 5th meeting, on 10 March, the panel discussion on the use of technology and trafficking in persons, smuggling of migrants and child abuse and exploitation was led by the following panellists: Douglas Durán (United Nations Latin American Institute for the Prevention of Crime and the Treatment of Offenders) as keynote speaker; Jo Harlos and Amber Hawkes (Facebook); Phiset Sa-ardyen (Thailand Institute of Justice); Michele LeVoy (Platform for International Cooperation on Undocumented Migrants); Jane Annear (Australia); and Irakli Beridze (United Nations Interregional Crime and Justice Research Institute).

6. Statements were made by the representatives of Brazil, Italy and Philippines.

7. At the 6th meeting, on 11 March, the panel discussion on artificial intelligence and robotics, ethical considerations and international cooperation in criminal matters was led by the following panellists: Cheol-kyu Hwang (President, International Association of Prosecutors) as keynote speaker; Roderic Broadhurst (Australian National University); Irakli Beridze (United Nations Interregional Crime and Justice Research Institute); Luciano Kuppens (INTERPOL); Arisa Ema (University of Tokyo); Taegyung Gahng (Korean Institute of Criminology); Danka Hržina (Croatia); and Frances Chang (United States of America).

8. Statements were made by the representatives of Argentina, Canada and the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders.

Chair's summary

9. The first panel began with a keynote speech emphasizing that despite their legitimate use, cryptocurrencies and other encryption technologies also present challenges in investigating online offences. Moreover, criminals continued to use virtual assets to move and conceal illicit funds, in particular in jurisdictions lacking anti-money laundering requirements. One panellis highlighted the substantial increase in research over the last two decades relating to illicit market operations online, with more recent focus on drug-related cryptomarkets. Recent evidence suggested that an underground economy had developed also around identity theft and the sale of stolen data. Reference was made by two panellists to notable successes in coordinated takedowns of dark web markets. Other panellists referred to the spread of additive manufacturing (3D printing) of firearms; technology used to hide weapons, evade security controls and facilitate their transportation; and the threat of "hybrid-firearms".

10. In the ensuing discussion, several speakers provided an update on their countries' preventive measures, good practices, and legislative reform efforts in response to various challenges posed by the criminal misuse of information and communication technologies. Several speakers emphasized the importance of specialized cybercrime structures within prosecutorial and law enforcement authorities. Emphasis was placed on the need for focused training of competent authorities. A number of speakers echoed the need for inter-agency coordination and public-private partnerships in response to cybercrime challenges. It was noted that the prevention and investigation of cybercrime needed to consider the protection of human rights and fundamental freedoms, especially the right to privacy.

11. A number of speakers highlighted the importance of strengthening cooperation between national authorities and communication service providers to ensure the preservation of, and access to, data and facilitate timely responses to cybercrime

cases. Some speakers welcomed the establishment, in accordance with General Assembly resolution 74/247, of an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

12. It was also stressed that existing multilateral legal instruments, such as the Organized Crime Convention and the Budapest Convention on Cybercrime, were the foundation of effective international cooperation in preventing and combating cybercrime; and that the participation of civil society, the private sector and academics was essential.

13. Some speakers highlighted the added value of the open-ended intergovernmental Expert Group on cybercrime – or a separate track within the UNODC framework in the future with due regard to the need for avoiding duplication - as a platform for the exchange of information on national and international responses to cybercrime.

14. The keynote speaker and panellists on the second panel noted that, while the rapid use of digital technologies worldwide had provided significant benefits to society, new opportunities for exploitation in relation to trafficking in persons and smuggling of migrants had emerged through the Internet and the use of social media and online gaming sites. The COVID-19 pandemic had exacerbated related criminal threats. One panellist highlighted that technology could be harnessed to improve gender-based responses, including by supporting remote investigation to reduce secondary victimization. Tracking illicit financial flows could be another way in which technology (such as blockchain and AI) could support anti-trafficking policies.

15. Two panellists referred to their company's approaches to online safety through prevention (e.g. safety notices and removing accounts that engage in potentially inappropriate interactions with children), detection (reducing harmful content; proactive detection; network disruption) and related responses (blocking fake accounts; collaboration with law enforcement authorities; help centres to report content related to trafficking in persons). Another panellist expressed caution about the growing use of digital technologies in border control and immigration. Two panellists referred to the emerging threat of the commissioning of livestreamed child sexual abuse.

16. In the ensuing discussion, multi-stakeholder strategies were identified by a number of speakers as a vital preventive element in the fight against cybercrime. One speaker supported the collaboration with national immigration authorities and international organizations to gain a better understanding of the virtual modus operandi of human trafficking networks.

17. The third panel started with a keynote speech referring to the advantages of combining artificial intelligence with direct contacts of authorities responsible for international cooperation in criminal matters. One panellist examined the role of the transparent use of artificial intelligence in judicial decision-making, as well as in forensic analysis, intelligence-led policing models and existing surveillance systems. One panellist referred to the UNICRI Centre for artificial intelligence and robotics, established with the aim to improve the knowledge of both the risks and benefits of such technologies. Another panellist presented the work of the INTERPOL Innovation Centre, aimed at assisting law enforcement authorities to keep pace with innovative policing issues.

18. Two panellists shed light on ethical considerations in the use of artificial intelligence. One of them noted that the academia could play an important role in research and education of researchers and practitioners. Another panellist underlined the potential conflicts with human rights of the use of big data and AI to predict crime. Therefore, related ethics guidelines were necessary to ensure efficient oversight, compliance with due process, fairness, non-discrimination and accountability. One panellist referred to challenges and lessons learnt from the impact of the COVID-19 pandemic on international cooperation in criminal matters, with reference to

adaptations and use of innovative approaches (electronic transmission of requests, videoconferencing, strengthening of direct communication and judicial networks). Another panellist underlined the importance of fully equipped and empowered central authorities, referring as good practices to the posting abroad of law enforcement and judicial attachés and the use of law enforcement channels prior to the submission of mutual legal assistance requests.

19. In the ensuing discussion, speakers reiterated the importance of strengthening international cooperation, including through the use of liaison magistrates. One speaker referred to examples of constantly evolving technological tools in national investigations. One speaker questioned about existing cases on admissibility and credibility of data obtained through artificial intelligence. In response, it was noted that this issue would be considered in the future and that tools for such consideration existed in domestic laws and multilateral instruments (provisions on the use of special investigative techniques and conditions thereof).

20. Further support was expressed for the UNODC Global Programme on Cybercrime, as well as the tools developed by UNODC, such as the SHERLOC management portal, the Directory of Competent National Authorities, the Practical Guide for Requesting Electronic Evidence Across Borders and the Mutual Legal Assistance Request Writer Tool.

21. The Chair invited participants to consider the following points raised during the discussions:

- (a) Combining geographic insights from cryptocurrencies with on-chain data reveals trends that mirror findings also reported in the “mainstream” drug trafficking market. On the other hand, more knowledge is required on how darknet market operations intersect. For better operational results, law enforcement authorities should develop synergies with various stakeholders, including the private sector and security researchers, with a view to supporting online investigations;
- (b) Member States should assess the need for a policy on the possession of, and trafficking in, blueprints for 3D printing that could enable illicit manufacturing of essential components of firearms;
- (c) Support was expressed for the application of new technologies for marking of firearms, record-keeping, tracing and destruction of designated arms. The need was highlighted to keep pace with technological developments, which may apply to multiple areas, to prevent the unlicensed production of firearms, their illicit conversion and reactivation, diversion practices and online trafficking in firearms;
- (d) Consideration should be given to the adoption of new technologies for stockpile management and security in the field of firearms, as well as for the use of new technologies for inventory management and the monitoring and protection of weapons in transit;
- (e) Member States should prevent corruption and increase transparency mechanisms, also building on the important role of industry, academic and civil society organizations on firearms and technology-related security threats, for example through increased cross-checking of databases, the use of big data and of new technologies for improved security of digital documents, and transparency in authorized trade;
- (f) Anonymous reporting of trafficking in persons and the submission of electronic evidence by citizens via mobile or internet platforms could be promoted to ease the work of authorities with limited manpower and resources;
- (g) Cloud-based technology, big data and artificial intelligence could improve technical capabilities for more effective and coordinated policy responses to trafficking in persons at the national and international levels;

- (h) Member States should closely review the implications for at-risk groups of the use of technology in policing and immigration control; and develop clear guidelines and ensure transparency in the use of technology in the context of immigration enforcement, while creating accessible means to challenge its misuse;
- (i) Member States should ensure that legislative frameworks sufficiently cover livestreamed child sexual abuse. There is also a need to further analyse how national data and intelligence can be utilized to detect indicators of livestreamed abuse; and also engage with digital industry and the financial sector to identify means for proactively detecting livestreamed abuse and ensure its reporting to law enforcement authorities;
- (j) Member States should ensure that legal frameworks keep pace with technological developments, including in relation to artificial intelligence, and should further seek to streamline international cooperation in criminal matters through the use of technology and innovative tools for use by practitioners and central authorities that are equipped and empowered to fully benefit from such use;
- (k) Member States are encouraged to monitor and understand the risks posed by the malicious use of artificial intelligence technologies to ensure accountability and integrity, promote ethical standards in using these technologies, and secure the confidence and trust of citizens and communities in the application of new technologies.