



UNODC

United Nations Office on Drugs and Crime

Fourth meeting of the Core Group of Experts on Identity-related Crime (Vienna, Austria, 18-22 January 2010)

I. Opening of the meeting and adoption of the agenda

1. The fourth meeting of the core group on identity-related crime was convened by the Chairman, Ambassador Eugenio Curia, representative of the Government of Argentina in Vienna, on 18-22 January 2010. The meeting was based on a multi-stakeholder concept and, in addition to the Chairman, the following experts representing different stakeholders attended it:

- a. Public sector:** *Christopher Ram*, Counsel, Department of Justice, Criminal Policy Section, Canada (Rapporteur of the core group); *Jonathan Rusch*, Deputy Chief for Strategy and Policy, Fraud Section, Criminal Division, Department of Justice, United States of America; *Christiane Rouma*, General Councillor, National Register of Physical Persons, Belgium; *Luc Vanneste*, Director General Institutions and Population Home Office, Belgium; and *Edwin Delwel*, Police Commissioner, Programme Manager ID Issues, Dutch Police, Netherlands.
- b. Private sector:** *Anko Blokzijl*, CEO, Sagem Identification, Netherlands; *Ferdinand Piatti*, Price Waterhouse Coopers, Austria; *Laurent Masson*, Director for Anti-Piracy and Internet Safety Law and Corporate Affairs - Europe Middle East and Africa, Chief Privacy Advisor for Europe, Middle East and Africa, Microsoft; and *Pat Cain*, Resident Research Fellow, Anti-Phishing Working Group (APWG).
- c. International organizations:** *Kate Lannan*, Legal Officer, International Trade Law Division, UNCITRAL Secretariat; *Demosthenes Chryssikos*, Crime Prevention and Criminal Justice Officer, UNODC Secretariat; *Justice Tettey*, Chief, Laboratory and Scientific Section, PARB/DPA/UNODC; *Barbara Remberg*, Scientific Affairs Officer, Laboratory and Scientific Section, PARB/DPA/UNODC; *Magali Bernard*, Associate Expert, Laboratory and Scientific Section, PARB/DPA/UNODC; and *Rebecca Bucht*, Laboratory and Scientific Section, PARB/DPA/UNODC.
- d. Academia/Individual experts:** *Marcos Salt*, Professor of Criminal Law, University of Buenos Aires, Argentina; *Gilberto Martins de Almeida*, MARTINS DE ALMEIDA Advogados, Brazil; *Marco Gercke*, Professor of Criminal Law, University of Cologne, Germany; and *Cormac Callanan*, Managing Director, Aconite Internet Solutions Limited, Ireland.

The following additional experts in forensics joined the meeting for the **session on forensics**: *Seong-Jin Choi*, Director, Digital Forensic Division, South Korea; *Meredith Dekalb Miller*, Forensic document examiner, Meredith Dekalb Miller & Associates, United States of America; *Larry Depew*, President, Digital Forensics U.S. LLC, United States of America; *Steve Hopkinson*, Chief Immigration Officer, National Department Fraud Unit, Intelligence Directorate, U.K. Border Agency, United Kingdom; *Marie-Blanche Langlois-Peter*, Head, Documents and New Technologies Section, Forensic Science Laboratory (Police), France; *J. T. Mothoa*, Director, Section Head, Questioned Document Unit, Forensic Science Laboratory, South African Police Service, South Africa; and *Sergey Potseuluy*, Ukraine.

2. The Chairman began proceedings by reviewing developments since the last meeting of the core group. The most important of these was the adoption by the Commission on Crime Prevention and Criminal Justice, and subsequently by the Economic and Social Council, of new legal mandates.¹ These mandates referred for the first time specifically to the core group and its work. In its resolution, the Council clarified the work and priorities of the core group by encouraging Member States to take action against economic fraud and identity-related crime and calling on UNDOC to provide assistance, as appropriate.²

3. The Chairman also reviewed some highlights of the thematic discussion on “economic fraud and identity-related crime”, held during the eighteenth session of the Commission on Crime Prevention and Criminal Justice in April 2009.³ The Chairman then suggested some ways in

¹ E/RES/2009/22 of 30 July 2009.

² The ECOSOC encouraged Member States, taking into account the recommendations of the Study on Fraud and the Criminal Misuse and Falsification of Identity (E/CN.15/2007/8 and Add. 1-3), to: combat economic fraud and identity-related crime by ensuring adequate investigative powers and, where appropriate, by reviewing and updating the relevant laws; develop and maintain adequate law enforcement and investigative capacity to keep abreast of and deal with new developments in the exploitation of information, communications and commercial technologies in economic fraud and identity-related crime, including websites and other online forums used to facilitate trafficking in identity information or documents, such as passports, driving licenses or national identity cards; consider, where appropriate, the establishment of new offences and the updating of existing offences in response to the evolution of economic fraud and identity-related crime, bearing in mind the advantages of common approaches to criminalization, where feasible, in facilitating efficient and effective international cooperation; strengthen international cooperation to prevent and combat economic fraud and identity-related crime, in particular by making full use of the relevant international legal instruments; develop an approach for the collection of comparable data on the nature and extent of identity-related crime, including, where feasible, from the victim’s perspective, that would allow the sharing of data among appropriate law enforcement entities and provide a central source of data at the national level on the nature and extent of identity-related crime, taking due account of national law; study, at the national level, the specific short- and long-term impact of economic fraud and identity-related crime on society and on victims of such forms of crime and develop strategies or programmes to combat those forms of crime; and adopt useful practices and efficient mechanisms for supporting and protecting victims of economic fraud and identity-related crime and, to that effect, enable effective cooperation between public and private sector entities through computer emergency response teams or other mechanisms providing an emergency response capability to public and private organizations requiring technical support and advice during periods of electronic attack or other network security incidents.

In addition, the Council requested UNODC to collect, develop and disseminate: Material and guidelines on the typology of identity-related crime and on relevant criminalization issues to assist Member States, upon request, in the establishment of new identity-based criminal offences and the modernization of existing offences, taking into account the pertinent work of other intergovernmental organizations engaged in related matters; technical assistance material for training, such as manuals, compilations of useful practices or guidelines or scientific, forensic or other reference material for law enforcement officials and prosecution authorities in order to enhance their expertise and capacity to prevent and combat economic fraud and identity-related crime; and a set of useful practices and guidelines to assist Member States in establishing the impact of such crimes on victims; and a set of material and best practices on public-private partnerships to prevent economic fraud and identity-related crime.

UNODC was also requested to provide technical assistance, including legal expertise, to Member States in reviewing or updating their laws dealing with economic fraud and identity-related crime in order to ensure that appropriate legislative responses are in place.

³ The salient points of the thematic discussion were as follows: (a) New forms of fraud and identity-related crime have emerged as a result of the spread of modern information and communication technologies: There is a need for new strategies and proper counter-action to tackle them; (b) It is essential to develop precise and detailed definitions and typologies to identify the contours of the crimes under discussion with a view to covering the widest possible range of conducts involved, especially those committed within “the life cycle” of identity-related crime; (c) The links and relationship between fraud and identity-related crime, on the one hand, and other crimes, on the other, such as transnational organized crime, corruption, cybercrime and money-laundering were emphasized: there is a need to enact and/or update domestic laws of Member States to reflect those links and provide for adequate legislative responses, as appropriate; (d) In considering the need to adopt and implement effective legislative measures to curb identity-related crime, different national approaches were discussed, ranging from the criminalization of identity abuses *per se* to the establishment of identity-related crimes within more general offences. As identity-related crime continues to grow as an international problem, it will become even more important in future for Member States to review the adequacy of their laws and, where appropriate, consider amending them, or enacting new laws, to ensure that they provide sufficient scope of coverage and appropriate criminal sanctions; (e) It is necessary to adopt and implement measures supportive to criminalization. Such measures include, for example, the establishment of flexible jurisdictional bases, extended

which the ECOSOC resolution would affect the ongoing work of UNODC and the core group, and the agenda of the present meeting. Noting that the next major step would be the forthcoming Twelfth Congress on Crime Prevention and Criminal Justice, to be held in Salvador, Brazil, from 12 to 19 April 2010, he suggested that the discussion be extended to possible ways of using this event as an opportunity to focus attention on the problems of economic fraud and identity-related crime and on the pertinent work of UNODC and the core group.^{4 5}

4. The members of the core group reviewed and adopted the provisional agenda of the meeting as the basic framework for the deliberations.

II. Agenda item 4: Typology and criminalization approaches to identity-related crime: Presentation of a draft manual – Compendium of examples of relevant legislation

5. Under this agenda item, two particular products in draft form were brought to the attention of the core group: a manual, still in primitive shape, to assist Member States in developing and drafting new identity-based offences and in reviewing and modernizing related existing offences; and a compendium of examples of relevant legislation on identity-related crime (and fraudulent practices linked to it) to be made available for use by Member States.

6. Mr. Gercke reviewed developments in legislation and international cooperation since the last meeting of the core group. He indicated that he had compiled examples of legislative approaches and guidelines on how States might use these in developing their own measures. There was a great variety of approaches noted thus far. Many States already had experience and had established some relevant offences, others had not. The approaches of States to identity-related crime were seen as more divergent than to some other forms of crime. The expert noted that, while each State would need to be comfortable with its own approach, it was still necessary

statutes of limitation and the use of new investigative methods and techniques. Particular attention should be devoted to the improvement and streamlining of criminal justice and law enforcement responses to address the evolving nature and complexities of the crimes under discussion, including both their conventional and on-line forms; (f) In view of the increasing transnationality of economic fraud and identity-related crime, the strengthening of international cooperation mechanisms is an indispensable component of the efforts to combat them effectively. It is important to foster new means of cooperation allowing for the exchange of information in real time. At the normative level, existing international legal instruments, including the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and, where applicable, the Council of Europe Convention on Cybercrime, provide a sufficient legal basis for international cooperation, and the focus of attention should be on efforts to promote the effective implementation of their provisions; (g) Special consideration should be given to the protection of victims of economic fraud and identity-related crime. Priority should be accorded to awareness-raising and educational programmes, the establishment of robust and efficient systems and processes of handling complaints and restoring, to the extent feasible, damages suffered, as well as to the improvement of coordination among competent national authorities involved in victims issues; (h) There is a need for appropriate preventive measures. Education and dissemination of information about fraud and identity-related crime to potential victims are critical elements of prevention strategies. Another major area is that of “technical prevention”, in the form of measures aiming at making information and other technologies more difficult for criminals to exploit and more protective of sensitive information; (i) Cooperation between the public and private sector is essential to develop an accurate and complete picture of the problems posed by the crimes under discussion, as well as adopt and implement both preventive and reactive measures against them; and (j) Priority should be accorded to the provision of technical assistance for building and/or upgrading the capacity of national authorities to address related issues, especially in developing countries and countries with economies in transition or in the course of reconstruction, rebuilding after conflict or natural disasters. With regard to specific forms of technical assistance, it is important to develop and keep up-to-date training materials for criminal justice and law enforcement officers, as well as persons who are in a position to identify and report relevant crimes.

⁴ E/CN.15/2009/CRP.10, /CRP.11, and /CRP.12 (reports), E/CN.15/2009/CRP.13 (criminalization) and E/CN.15/2009/CRP.14 (victims). Also disseminated was the paper on criminalization tabled by the G8 Lyon Group, E/CN.15/2009/CRP.9.

⁵ E/2009/30, paras. 5-31, available in all official languages on the web sites of UNODC, ECOSOC, and in the UN Official Document System.

to come up with a set of guidelines to support as many focused and common approaches as possible. On the one hand, laws needed to fit into domestic systems, but, on the other hand, most identity-related crime was clearly transnational in nature. Such crime could be committed locally, but the ease of transfer of data had made global trafficking much easier and more profitable for offenders and tended to be the norm. Thus, there was a need for harmonized or compatible legislation in support of better international cooperation. The expert raised the question whether Member States could live with such a diversity of legislation, and to what extent the development of models, standards or examples by UNODC could assist in obtaining greater standardization. In this regard, the core group noted that there were practical limits on how far materials should go and that materials in the nature of model laws, in particular, should be considered with caution.

7. In discussion, it was noted that, while there were differences between developed and developing countries⁶ and between common law and civil law systems (see below), all States recognized one common area, that of the need to have effective international cooperation. In the course of developing criminalization materials, for example, one key function, apart from assisting various States to develop appropriate offences, was to explain the needs and approaches of common law States to civil law States, and vice-versa. In that context, several experts noted that this would make the compilation and use of practical examples and information and classification based on offender methods important. While legal approaches might vary from State to State, offender methods were universal. More generally, there was agreement on the need to explain to Member States clearly the seriousness and nature of the problem, with a view to providing both motivation and direction in establishing appropriate criminal offences.

8. Related to this was the need to ensure that any new or modified offences meet the “serious crime” requirements of articles 2 and 3 of the United Nations Convention against Transnational Organized Crime (UNTOC) so that they could form the legal basis for international cooperation, where applicable. It was noted that, as a global instrument, the UNTOC was of necessity at a general level and that training materials on international cooperation could support the efforts of States to go beyond this in bilateral agreements or arrangements, where practicable.

9. The research on criminal offences was presented by Mr. Gilberto Martins de Almeida with a view to briefing the members of the core group on the structure and methodology of the compendium of legislation on identity-related crime. He reviewed a range of existing and proposed provisions from the laws of 28 Member States, which had been provided by members of the core group, Member States, and the G8 Lyon Group. The information was based on four basic questions as follows:

- Which national laws or types of law specifically address identity-related crime?
- Which categories of identity documents or information are protected by such offences?
- Which types of acts are criminalized?
- Within specific offences, what elements were used to establish the basis of the offence and limit its scope?

10. The full range of offences included in the research was considered, focusing on the need to limit the scope of offences and thereby avoid criminalizing innocuous conduct or creating overbroad offences. Examples included the taking of tangible documents, taking or copying of intangible data or information, the use of deception by commission (giving false information) or omission (providing incomplete misleading information), computer crimes, such as invading websites, and offences directed at the protection of specific documents, most commonly either passports or national identity documents. Also discussed were offences relating to the possession or use of software designed or intended for use in committing identity-related crimes, and offences related to the manipulation, transfer or trafficking in identity documents or identity information. Many States had established general offences, such as fraud, and offences protecting

⁶ Mainly technological differences, as well as differences between countries with centralized identity infrastructures and those with a more ad hoc arrangement.

specific forms of identification, such as passports, but most States had not gone far in the direction of developing specific offences dealing with abuses of identity *per se* in particular, as envisaged by the 2007 Report of the Study on “Fraud and the criminal misuse and falsification of identity” (2007 study). Some States had relevant offences based on offender methodologies, such as cybercrime offences based on specific abuses of technologies. Many of the countries examined had also enacted specific offences or aggravated offences or sentences for the purpose of enhancing deterrence and adding additional protections for particularly vulnerable or important forms of identification, or where there were indicia of more serious criminal offending. A trend identified, for example, was that of the establishment of aggravated or more serious offences for tampering with public sector identification. Transnationality of identity-related crime could also be an aggravating condition. Mr. Almeida expressed the view that, while there were still relatively few specific identity crime offences, the range and complexity of related offences was such that it would be very difficult to carry out a gap analysis. It was also noted that such an analysis would be complicated by the many definitional and boundary issues, such as the overlaps between identity crime and most forms of fraud and the grey areas between identity information and other forms of personal information identifying an individual.

11. A range of specific issues relating to the formulation of offences in different types of jurisdiction were further discussed by the core group. It was noted, in this regard, that one of the most significant challenges in formulating new offences was to find definitions and terminology to ensure that the desired socially-harmful conduct was criminalized, while at the same time avoiding offences which were too broad and might include innocuous, trivial or justifiable conduct.

12. It was further noted that different approaches were used in common law and civil law jurisdictions. Civil law systems, on the one hand, treated the definition of offences as an issue of legality, in that vague or overbroad definitions were not considered to be in conformity with the Roman axiom *nullum crimen nulla poena sine lege certa*. Common law systems, on the other, tended to treat the limits in defining related offences as infringements of rights, such as the right to be faced with clear and precise allegations to which one could respond. Common law systems had more flexibility in drafting initial offences, since the exact application of a general offence provision could be left to judicial interpretation and application to specific facts.

13. Furthermore, a key issue between common law and civil law States was the tendency of the latter to rely more on liability for identity abuses as preparation for other crimes, such as fraud, where the former were more likely to create separate offences, even if there was some degree of overlap. The civil law approach entailed greater restraint in the application of the criminal law and limited the creation of redundant offences. On the other hand, the common law approach provided more possibilities of a successful prosecution in certain cases. For example, in cases where a scheme could not be established, or where identity elements were committed by one actor and other elements such as fraud or illegal use of identity documents were committed by others after the documents had been trafficked, all of the participants would be included in specific identity crime offences.

14. At a more general level, both civil law and common law systems had faced the basic need to limit the scope of offences and provide sufficient precision and clarity, and the means used by both to accomplish this were discussed. Apart from the use of definitions and clear drafting, among the more common means of limiting scope was the use of mental elements or requirements of intent or purpose. Intent elements were often applied to accused offenders, and purpose elements to tangible devices, such as machines, or intangible ones such as software. For example, a State might criminalize possession of a device designed for the purpose of phishing data or skimming credit card information, with knowledge that the “device” had such a purpose and/or the intent to so use it. Another common limit was the use of exclusions for cases where there was consent, lawful justification or some other condition which rendered otherwise-harmful conduct innocuous. Definitional provisions were often used to specify and limit the types of data or document protected. Some States dealt with “identity information” *per se*, while others dealt

with it under more general protection as a form of “personal information”, within which other types of personal information, such as health or financial information were also included. What was done with identity documents or information was a common basis for offences. As for the conduct targeted, it usually involved acts such as taking, copying, falsifying or fabricating identity information, but some provisions took the opposite approach, being based on the nullification, removal, deprivation or vitiation of identity, in the sense that the offence was based on damage to the victim of the crime as opposed to the undue advantages gained by the offender.

15. In discussion, it was noted that one strategic need for the development of technical assistance materials would be to provide guidance to Member States on how they could establish crimes broad enough to address the full scope of the problem and at the same time provide them with a range of options for circumscribing the offences to avoid over breadth, legality, human rights and constitutional problems, and also to avoid practical problems with domestic investigations and international cooperation. It was also stressed that there was a need to distinguish between minor transgressions and more serious crimes, and a number of specific criteria were discussed. Usually these focused either on the seriousness of the crime in terms of harm to victims or society, or on the obstacles encountered by States in preventing, investigating or prosecuting relevant crimes. Elements considered, in this context, included the involvement of organized crime, links to other serious crimes and elements of transnationality. Other criteria were more practical: States might have offences relating to the possession or transfer of documents that were triggered or aggravated if certain types, or more than a certain number, of documents were dealt with, an approach similar to drug offences where the possession of large volumes triggers an inference that possession was for the purpose of trafficking. Where a suspect is apprehended in possession of a large number of passports, for example, it is likely that some form of serious identity crime, or a related offence such as trafficking in persons, is involved.

16. The Chairman noted that a key question for the core group and for UNODC would be how to apply these diverse criteria to focus on a more uniform global approach. Several ways of grouping, sorting and presenting the criteria were discussed. They would generally need to be made accessible to common law and civil law States, to States at high and low levels of technical development in their national identity infrastructures, and to States with both centralized and *ad hoc* identity infrastructures using commercial and subject-specific identity documents. One possibility was to develop a “core list” of elements useful to all types of State and then more specific additional lists of elements primarily useful to each different type. Typologies based on legal criteria and contexts could be very specific, whereas typologies based on offender conduct – which was universal – had the advantage of being equally applicable to all types of legal system and context, but were less specific in suggesting legal responses. There was general agreement that offender-based provisions would be more standardized, thereby forming a better basis for international cooperation. It was also agreed that offences, to ensure clarity and avoid overbreadth, would need to use mental elements and factual distinctions. Some experts also noted and there might be a need for offences of lesser severity to provide options for dealing with less-serious conduct and that many States already had regulatory or other non criminal options for this. They also noted that a specific threshold of seriousness was needed to trigger application of the UNTOC.

III. Agenda item 5: Protection of victims: Useful practices and guidelines

17. The core group noted that there was a clear mandate for UNODC to develop guidelines for States on how to assess the impact of identity-related crime on victims.⁷ However, there was not as much information available to the group as for issues relating to criminalization and

⁷ E/RES/2009/22, subparagraph 7(c).

international cooperation. The primary question for UNODC and the core group was to examine how to proceed with this issue.

18. There was general agreement that more information was needed, and that this would take longer than for the other two issues. It was noted that almost all of the available data came from the United States, which might not shed much light, especially on issues arising in developing countries. Some practical issues relating to the gathering of such data were discussed, including the question of sampling errors in data gathered on-line, and differences in the approaches of the public and private sectors. The general consensus was that there was a need to obtain more broadly based data, including from the private sector, to the extent it could be obtained. Several members agreed to conduct their own searches in several languages. One expert noted that it would be necessary to formulate specific questions for companies and that the opinions of those in companies dealing with victims would also be an important source of information.

19. There was some discussion of whether there was a need to examine regional differences in victimization, and, if so, whether it would be possible to obtain appropriate experts and data. In this context, it was suggested that a regional assessment of victims issues might focus, for instance, in the Latin American region.

20. The possibility of a future core group meeting supplemented by experts in victims issues was also discussed. There was general agreement that such a meeting should be held in late 2010 or early 2011, with the core group supplemented by victim experts, and that the expanded group should be supplied with a document for discussion. This document should contain a summary of the available data, some analysis of the data and its strengths and weaknesses, and a draft list of best practices for dealing with victims. Invited experts should also be sent a list of questions and asked to bring as much information as possible to the meeting. To the extent feasible, the victim experts should be chosen with regard to equitable geographical representation.

IV. Agenda item 6: International cooperation: Presentation of a draft manual for use by investigators and prosecutors

21. Under this agenda item, Mr. Gercke presented the results of his research for the purpose of elaborating a manual for use by investigators and prosecutors in the area of international cooperation to combat identity-related crime. He noted that one of the objectives was to make the manual accessible to law enforcement and other personnel confronted with international or cross-border identity offences, but with little previous experience in international cooperation. Mr. Gercke emphasized the great support of the co-author responsible for the practical aspects of the manual, Mrs. Raluca Simion, Ministry of Justice in Romania. Key questions in the drafting exercise revolved around the transnationality of the offences under consideration, whether they were “serious crimes” and whether organized criminal groups were involved, as required by the UNTOC. The potential of a range of regional and bilateral treaties, agreements and arrangements, including the Council of Europe Convention on Cybercrime that was ratified by 26 European countries and one non-European country, was discussed. The expert noted that the Council of Europe Convention on Cybercrime did not appear to have been used much, if at all, in identity-crime cases as the Convention did not specifically criminalize identity-related crime. A further question was the nature of international cooperation where no legal basis to facilitate it was available (e.g., based only on reciprocity).

22. The expert clarified that, for the purpose of elaborating the manual, a format based on the use of sample cases was chosen. This involved the selection of sample cases composed of typical elements that tended to arise in identity crime cases. The cases also included examples of the use of central diplomatic channels and some of the more expedited or more direct means used for cybercrime offences, given that identity crime cases often involved on-line or internet offences,

and that fast responses were often critical in such cases. The content of each case included parameters such as the criminal conduct involved, the nature of the transnational elements, and differences in the legal systems of the States involved. Strategic elements included setting out which instrument(s), if any, might be applicable or available based on the States involved and the nature of the facts. Different factual elements might apply for cases within Europe or among Parties to the UNTOC, for example. Advice included both practical measures and basic legal requirements, cross-indexed to other on-line resources with additional materials on the instruments that could be reviewed if users required additional information. The examples also examined the differences between formal requirements and practical needs and highlighted means of achieving expedited cooperation, where needed. The basic concept was to enable prosecutors to identify critical facts, understand why they were important in legal or practical terms and provide suggestions as to how to deal with them. It was suggested that an additional case-study on joint investigations be inserted in the manual.

23. There was discussion of the differences between formal and informal cooperation, and the various circumstances where informal cooperation could be used to expedite cases or facilitate rapid cross-border investigative measures needed to preserve evidence. It was noted, in this vein, that it would be useful to consider how informal networks or channels could be used for the sorts of cooperation envisaged. For example, informal cooperation was often used to obtain basic information in order to establish the need, basis and scope for more formal cooperation requests. Such basic information would usually not trigger formal legal requirements and the core group put emphasis on this.

24. One critical issue was to ensure that investigators and prosecutors could distinguish between information that required formal legal procedures, and information which could be obtained more directly, such as information publicly available in another State. A key message was to inform law enforcement that effective international cooperation was feasible in identity crime cases and could be made to work. There was otherwise a risk that inexperienced national law enforcement would be discouraged from taking up cases to begin with. It was noted that a methodology based on case studies offered many of the same advantages as with the criminalization issues. First, because it was a good means of explaining complex requirements to investigators in practical terms; and, second, because it would in general be equally applicable to common law and civil law systems. Also discussed were the possibilities offered by “24/7” systems. It was suggested that these might prove effective, but were only a means of communication and did not address the fundamental legal and sovereignty issues. It was further noted that they might possibly prove more effective if information were shared as intelligence rather than evidence, in the manner that the Egmont Group coordinated the sharing of information related to money-laundering among national financial intelligence units.

25. There was also discussion of the basic scope of the international cooperation materials. It was noted that, on the one hand, that was a term of art which referred specifically to the transfer or sharing of information for use in investigations or as evidence, which would generally trigger a requirement to consider formal channels and safeguards. On the other hand, in a more practical sense, there were forms of cooperation, such as the sharing of expertise or tools, which were outside of the scope of the term of art. The question raised was to what extent materials directed at investigators or prosecutors needed to deal with the broader issue. One possibility was to distinguish between information which was not investigative, such as the sharing of investigative techniques, information which was investigative but was openly available and did not trigger international cooperation safeguards and, finally, information which engaged sovereignty, human rights or similar issues and therefore did trigger the need for mutual legal assistance and similar international cooperation safeguards.

26. The sharing of information obtained from private sector entities was also examined. It was noted, in this regard, that generally private sector entities had the technical means to locate stored information or intercept communications quickly. However, the lack of criminal law or constitutional oversight on the private sector entailed the risk of circumventing human rights or

other fundamental safeguards, and therefore the ability to use information obtained from the private sector in criminal prosecutions was limited. Several experts noted, on the other hand, that the capabilities of the private sector could still be very useful. Some forms of basic information did not trigger the need for protections and could be shared without much restriction, and more sensitive information could be “frozen” to prevent automatic or deliberate erasure pending formal mutual legal assistance requests. It was noted that this issue was common to the investigation of most forms of cybercrime and had been a difficult issue during the negotiation of the Council of Europe Convention on Cybercrime.

27. The question of ensuring that materials would apply to cases between common law and civil law countries was discussed. It was not seen advisable to go into too much detail as to the differences between common law and civil law systems, but it was recognized that there might be some need to inform investigators about the basic differences, and how some of these could be minimized so as to ensure that foreign requirements would be met.

V. Agenda item 7: The role of the private sector in the fight against identity-related crime – Presentation of an inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime

28. Under this agenda item, a paper including an inventory of best practices regarding synergies between the public and the private sector to prevent economic fraud and identity-related crime was presented by Mr. Callanan. This paper examined issues not only limited to identity-related crime, but also to organized crime and cybercrime, and further suggested that public-private partnerships could take many forms. It was noted that public sector entities did not sometimes fully understand the position or capacities of the private sector and that the expectations placed on companies were sometimes too high. In addition, the private sector had to remain commercially viable and therefore business and State objectives or agendas did not always coincide. Companies also faced other countervailing pressures, such as human rights of subscribers. The paper recommended that much could be accomplished by focusing on shared interests of both the public and the private sectors, especially in the early identification of crime and in educating new subscribers.

29. A number of factual and statistical figures were reported, covering both cybercrime and identity-related crime committed using information and communications technologies. For example, on-line worms and other hostile software were now prevalent on-line, to the point where unprotected new machines on-line were usually attacked within first 30 seconds. In the most recent year for which statistics were available, there were an estimated 10 million U.S. victims and about 1/10 of U.S. users were victimized. About 18% did not find out about an identity theft for 4 years. New rapid monitoring and reporting systems were now being developed and implemented. Identity theft insurance was for sale in the United States, and insurers might soon become a good source of information on both the scope of victims and the extent of the harm they suffered. Many problems were faced by victims in the course of resolving identity compromises, including the need to contact many different sources at home and abroad and difficulties establishing their own valid identities. 70% of victims reported that they had encountered difficulties in resolving the problem. Almost ½ (46%) of victims knew the perpetrator. About ½ of all cases involved paper thefts, and only about 11% were on-line, although about half involved digital information. The recent trend in online attacks had been to become much more focused to deal with, for example, specialized applications.

30. Available data suggested that specific threat categories differed significantly depending on region or country. Some threat patterns might differ depending on the target. For example, home and business users had different data and different software to protect it and were thus attacked

differently. There were some major fluctuations in occurrence rates, but these tended to be produced by technological changes and the interplay between ongoing offender behaviour and technical environments which could change abruptly.

31. In general, cybercrime was seen as a common adversary or challenge that could and should motivate cooperation between the public and private sectors, especially in view of crimes committed in virtual environment. It was stressed that such cooperation was fostered through technical anti-crime developments. It was noted, in this regard, that over the last years high-profile incidents and the fear of crime on-line had made security features and other anti-crime elements a new marketing tool for companies resulting in security innovations and improvements.

32. It was also underlined that many of the same jurisdictional issues confronted by investigators and prosecutors also plagued the companies themselves, and these included both factual and legal problems. Companies faced with search warrants might not themselves know where data was physically located, as it might be in more than one places or moving from one place to another.

33. The role of Microsoft as both a software company and service provider was highlighted during the meeting. It was noted that the company had developed some specific software for law enforcement, such as software used to track child pornography on-line, and was also engaged in training and capacity-building for law enforcement and other officials. The involvement of the company in cooperation on anti-fraud projects, such as an ongoing partnership with African development banks against advance-fee fraud, was also reported. It was stressed that a critical element for enhancing cooperation between the company and the public sector was the establishment of contacts that were not often rotated or reassigned to other positions.

VI. Agenda item 8: Technical assistance activities for capacity building: Identification of priorities and needs

34. The Chairman began the discussion of technical assistance issues by reviewing the new mandates set out in ECOSOC resolution 2009/22, paragraphs 7 and 8. He explained that most of the work needed to fulfill these mandates would be contingent on the availability of resources, both to prepare technical assistance materials and actually deliver projects. Some delivery would be organized and/or carried out by the secretariat, and there would also probably be numerous bilateral technical assistance efforts by experts from individual Member States. He also noted that some aspects of technical assistance might well fall within the ambit of technical assistance under the UNTOC. The Rapporteur noted that, in addition to the most recent and most specific mandates, much of the preparatory and technical assistance work would also fall under the earlier mandates in this field, calling for the use of information gained by the 2007 study, including the 2004 mandate to produce “useful practices, guidelines or other materials”, and the 2007 mandate to provide “...legal expertise or other forms of technical assistance...”⁸

35. In discussion, it was noted that both Member States and the private sector held much more relevant information and legislative precedents on economic fraud than on identity-related crime, but that much of it could probably be used, with appropriate modifications, for identity-related crime. There was general agreement that, for the most part, it should be possible to take training materials from relevant parts of fraud and adapt or supplement them for use in identity-related crime materials, thus building up a package gradually. Most forms, and most occurrences, of identity-related crime were also forms of fraud, and these could be supplemented with other forms as necessary. One advantage of this approach was the greater diversity of Member States having information on fraud. However, this depended, to some extent, on the nature or purpose of

⁸ E/RES/2004/26, paragraph 5, and E/RES/2007/20, paragraph 14.

the technical assistance, however. In dealing with investigative and forensic matters, for example, content would be similar. However, the mandates regarding criminalization were essentially to assist Member States to modernize existing fraud offences to respond to the criminal use of technologies, as well as increases in transnational and mass-frauds, and to assist with the establishment of entirely new offences dealing with identity-related crime. With regard to forensics, in particular, materials might be much more common, since types of evidence used in identity crime cases might involve paper documents, digital evidence, and other common forms of evidence or investigative techniques. Here the task would be to assemble, edit and compile into specific packages or practices information appropriate for identity-related crime, bearing in mind the different approaches to identification in developed and developing States (see below).

36. It was stressed that it would be important to take advantage of synergies and avoid any unnecessary duplication of effort. As with legislative materials, some investigative materials and materials dealing with evidence and international cooperation would also need to take account of the different offences and approaches to preparatory conduct in civil and common law States. Traditional modalities, such as compiling a library of resources and access points were discussed. Also discussed were more novel ideas, such as the creation of a roster of experts, and the idea of creating a consultative platform, although the latter may raise some concerns about the validity of information shared, especially with respect to legal and policy advice. Bearing in mind the strategic objective of encouraging Member States to pursue common approaches to criminalization there would have to be some control over content.

37. It was further noted that the compilation of information should take into account the factor of regional representation, to cover especially Africa, Asia and Latin America. In developing materials, representation from Africa could include Nigeria and South Africa, and from Asia, Hong Kong and Singapore might be good sources of appropriate expertise. From Latin America, Argentina and Brazil might further be taken into account for expertise resources. The work of, and expertise brought by, ITU were also stressed⁹ and a number of possible areas in which the ITU might have information or expertise that would assist the core group in its work were indicated. The option of establishing contacts with Interpol in search for further useful resources was also mentioned. One expert referred to the work of the European Union on digital evidence, as well as to the cybercrime Unit at the Organization of American States. The Chairman indicated that a priority should be to develop an inventory of materials and expert resource persons. The Rapporteur reiterated the need for modular and flexible materials, prepared in such a way as to be used alone or integrated into broader technical assistance programmes.

VII. Agenda item 9: On-line identity-related crime as a form of cybercrime: Feedback for the discussion at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice

38. Under this agenda item, the Chairman briefed the expert group on the forthcoming Twelfth United Nations Congress on Crime Prevention and Criminal Justice. He noted that a discussion of identity-related crime was envisaged as part of the agenda item entitled “Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime”. He also noted, however, that based on the discussions of the regional preparatory meetings for the Congress, the Congress debate itself was likely to be

⁹ Given its long standing experience in cybersecurity and cybercrime, ITU has launched a Global Cybersecurity Agenda and was entrusted by WSIS leaders to be the Facilitator and Moderator for WSIS Action Line C5 “Building Confidence and Security in the use of ICTs”. In addition, ITU, through its Development Bureau, provides technical assistance to developing countries and an ITU-T study group on Identity Management has been dealing with more technical issues.

dominated by the question of whether or not the Congress should recommend the initiation of a process which could lead to the elaboration of an international legal instrument on cybercrime. In this connection, there was some discussion of the issues that would be raised in such a process. Generally, members of the core group felt that the major issue would be whether the subject-matter itself was ripe for negotiation and thus whether the process of creating a new instrument should commence at all. Should such a process start, it was likely that the major focus of any potential instrument would be the establishment of basic offences and a framework for international cooperation, taking into account the unusual speed with which most forms of cooperation in cybercrime cases were required and the need to strike an appropriate balance among factors such as the respect for national sovereignty and the need to protect basic human rights.

39. Given that much of the Congress process was likely to be devoted to the question of whether to elaborate a cybercrime instrument, there was discussion of how the subject-matter of identity-related crime could be included and underlined. As the topic was to be dealt with in the Congress plenary and not at any of its workshops, the substantive framework of the discussions would be primarily in the form of interventions from Member States. In terms of legal substance, the core group noted that specific provisions with respect to identity-related crime, including criminal offences and specific forms of cooperation, if any, would be included, if at all, with other forms of crime committed using computer systems, possibly in the same manner as subjects such as trafficking in persons and firearms had been dealt with in the UNTOC. It was therefore suggested that members of the group urge their governments to include references to the issue in national interventions on this item. While members of the core group saw it as important that some of the work on identity-related crime be linked to cybercrime and brought within the scope of the Congress debate, they also noted that it was important not to conflate the two subjects entirely. In this connection, it was stressed that, while some forms of identity-related crime were linked to cybercrime techniques and information technologies, many forms were not, and that many of the Member States still relied primarily on paper documents as key elements of their identity infrastructures. It was therefore seen as important to include both aspects, while maintaining distinctions between them, and to ensure that a full range of experts were included in various discussions. In dealing with the full range of identity-related crime issues, members of the core group saw a need for the work of UNODC to address offences against both intangible electronic elements of identity and paper-based or other tangible elements. To a certain extent, this might entail the tailoring of materials or projects to suit that nature of national or regional identity infrastructures. However, it was clear that the use of information technologies and other high-technology means by offenders constituted as much of a problem for tangible infrastructures as did more traditional criminal techniques. In that context, materials and projects would need to address all aspects of the problem.

VIII. Agenda item 10: Session on forensics: The use of forensics to combat and prevent identity-related crime

40. The main objective of the session on forensics was to come up with a set of observations on the use of forensics to combat and prevent identity-related crime and recommendations on training and reference materials needed to assist law enforcement officials and prosecution authorities in their respective tasks. The Chief of the Laboratory and Scientific Section of UNODC provided some background on five decades of work of the Section, starting with narcotics analysis, and more recently moving into more general investigative areas. In essence, this work consisted of the development and use of materials to support forensic work in the form of standards and guidelines for Member States worldwide. While the issues relating to the scientific analysis of narcotic drugs and psychotropic substances were well-established, the expansion into non-drug areas of crime represented a formidable challenge because of the breadth

of the field and number of specific forensic fields. The Section had commenced with materials dealing with basic crime-scene procedures,¹⁰ and now sought to produce materials dealing with forensic issues associated with identity-related crime. This was seen as a priority for the Member States, as well as an area where forensic-support materials could usefully supplement the ongoing work of the secretariat relating to criminalization, international cooperation and technical assistance. The primary objective was to produce a single global standard and set of practices to assist Member States, and to support, to the extent possible, common approaches to the gathering, production and forensic analysis of evidence, as well as its production in judicial proceedings and its sharing with other States. It was noted that the envisaged materials were expected to target a range of audiences, including policy makers, educators, prosecutors, forensic experts, and front-line investigators.

41. The secretariat (Laboratory and Scientific Section) summarized the content of a draft discussion paper on “The use of forensic to combat and prevent identity-related crime” and reviewed the agenda for the forensics discussion. It was indicated that there was a need to identify necessary materials, clarify what was already available, identify gaps and discuss how to address them. The secretariat hoped to derive from the meeting some guidance from the core group as to how they should proceed in future. Mr. Depew, who was in charge of drafting the discussion paper referred to certain key elements and challenges, such as identifying the juridical and criminological nature of identity-related crime; discussing the types of physical evidence likely to be encountered; and identifying the relevant forensic disciplines and their potential contributions and limitations with respect to identity crime investigations. He indicated that, as with other activities, the lack of concrete information about the nature, scope and volume of identity-related crime presented some problems for forensics. He also reviewed the basic range of criminal conduct and probable offences that would have to be supported, often in the context of the investigation of fraud and other offences commonly associated with identity abuses. There was further discussion on the meaning of the term “physical evidence”. Generally, it was noted that this was used by UNODC (and in the present report) to distinguish between physical evidence obtained by investigators and subjected to forensic analysis, as opposed to opinion or other expert testimony before the courts as to what physical evidence meant. It was not intended to distinguish between tangible evidence such as documents and intangible evidence such as digital data. Thus, for example, data and the storage media on which they were stored could be considered “physical evidence”, whereas the opinion of an expert as to the nature or origins of such data would not.

42. The consultant also reviewed the possible range of types of physical evidence, including physical documents and digital storage devices and why each was important. He indicated that documents and data could be used to establish the basic nature of an item, but also a course of conduct or legitimate illicit activity critical to the success of a prosecution. Evidence such as records of computer communication could be just as important as documents, in effect to provide context, evidence of motive or other facts that would support evidence from other sources. Different scenarios relating to the falsification and fraudulent use of false or genuine documents were also discussed. From a forensic standpoint, making or altering documents could involve traditional forgery instruments and methods, and increasingly digital equipment such as scanners and printers, as well as transactional data.

43. The consultant further reviewed accreditation issues. It was noted, in this regard, that it was necessary to develop tests and practices for the processing and analysis of evidence that produced reliable results, but also to accredit labs and experts in order to ensure that their analysis would be acceptable in court. Certification could become a particularly critical issue in transnational prosecutions, where experts from one State might have to appear before, or submit evidence to, the courts of another.

¹⁰ See *Crime scene and physical evidence awareness for non-forensic personnel*, ST/NAR/39, UN, NY, April 2009, <http://www.unodc.org/unodc/en/scientists/crime-scene-awareness.html> (E/F/S).

44. Some of the aspects of forensic analysis and the uses to which such analysis could be put were also reviewed. Analysis of tangible documents often followed the basic production process, commencing with basic elements such as papers, inks, printing techniques and the specific anti-forgery elements that were increasingly included, especially in secure documents such as passports. Such documents might also contain data elements such as optical codes or chips containing further or collaborative information, or linking the document with information stored elsewhere. After analysis of fundamental elements such as papers, inks and binding methods, the next steps usually involved items added later, such as signatures, and then to subsequent alterations or other tampering, if any. Basic forensic analysis started with front-line workers, such as passport officers, and progressed to more sophisticated environments when crime or falsification were suspected as a result of the initial observations or for other reasons. While forensic analysis was usually done to support specific investigations and establish whether documents were authentic, it was noted that it also served broader and more systemic purposes. Forensic analysis often identified new criminal techniques or trends that could be used to detect criminal operations, brief immigration officers, law enforcement officers or other target groups, and to assist those charged with producing documents and related systems to make them more difficult to falsify or subvert. It was stressed that in criminal cases, the first step was to determine basic authenticity, and if not authentic, then to determine what had been falsified or altered, how, and by whom. In this context, some of the forensic techniques and instruments were mentioned, including spectral analysis, microscopes, specialized lighting techniques, spectroscopy and other methods that could be used to detect or establish the false or fraudulent nature of various documents.

45. The implications of this for the development of technical assistance materials were then discussed. The core group felt that the nature of the information and range of target audiences would make it advisable to produce a range of materials, varying in detail depending on the degree of sophistication of the target audience. There would be a need for materials directed at forensic experts, other investigators, judges and prosecutors, law enforcement in general, administrative officials in charge of examining documents, such as passport or immigration officials, as well as other groups. Part of the exercise would have to involve determining the needs of each target group. Another would lie in bridging the gaps between them, in the sense that materials could explain the functions and limits of one group to another. The core group also felt that the development of specific modules that could be used in isolation, as part of larger forensic exercises, or in the context of other anti-crime or other technical assistance projects would best ensure the effective use of the information, while keeping any duplication of effort to a minimum.

46. One expert noted that the field was becoming increasingly difficult, in the sense that large numbers of lower officials needed more and more sophisticated training and access to detection materials, posing the challenge of how to deliver information to such officials so that they could readily access and use it on a front line basis. Another expert argued that materials would need to be used in both a reactive and preventive context, and that those in the best position to prevent abuses were often most remote from the latest developments in forensics. Part of the agenda was also to reverse some assumptions in order to reach those producing and issuing high-risk documents. Educating, for example, those in charge of issuing drivers licenses would be different from reaching those checking passports. It was also noted that part of the problem would be to disseminate information, not only about criminal techniques in general, but about a range of authentic documents and specific types of forgery. This could include very large numbers of specific documents. While information about various passports was disseminated internationally, there was at present little, if any, access by the officials of one State to the identity documents of other States to assist in identifying forgeries. Even within some States, the same basic identification document might take many forms, as changes to basic forms were made over the years to make forgery more difficult. This depended, to some degree, on the length of time for which documents remained valid and whether older forms were replaced with new ones when documents expired. It was noted, in this vein, that developing a global inventory of documents

would pose a major challenge, but that it should be possible to provide Member States with the basic characteristics so that each could maintain its own database. It was argued that this was a possible output for UNODC, which could provide assistance in establishing such databases and in sharing the information on them in transnational cases. It was also stressed, however, that the scope of such a project might go beyond that of the UNODC or any other specific international organization, given the range of non-criminal uses to which such a database could be put.

47. In terms of the use of forensic materials in prevention, it was underscored that it was important to ensure that basic document forms and identity infrastructures needed to make the rapid identification of false or suspicious documents by front line officials as efficient and effective as possible. Sophisticated technologies for detecting forgeries could only be used on a limited number of documents in major cases. At the other end of the spectrum, facilitating the mass-screening of large numbers of documents was also necessary. This made it important to provide those producing documents with the means of developing innovations against the latest criminal techniques, but also to incorporate elements that would make falsification or tampering easy to detect by front-line staff using only visual observation or very basic technical apparatus.

48. The means of identifying digital data and establishing continuity, which were different from those used for tangible documents, were further discussed. Continuity, namely the task to ensure that the proof that evidence produced in court was the same evidence actually recovered by investigators and linked to accused offenders, was more difficult in the case of digital evidence because of its intangible nature. In this vein, the concept of “hash values”, based on calculations that were specific to an individual file, was explained. Once the identity of data was established, continuity often involved the use of secure data storage archives and storage media to facilitate proof that electronic evidence presented in court was authentic and had not been tampered with. Operational forensic methods for dealing with data were further discussed. These included basic computer workstations and equipment which could copy data while embedding elements to establish continuity and authenticity. It was noted that this was a rapidly-evolving area in that this sort of information would have to be frequently updated in any training or technical assistance materials. The copying of data normally involved various forms of compression to edit out redundant or meaningless elements, but for forensic purposes, the “imaging” of data, in which there was no compression or modification in storage or transmission, was required. There was also discussion of issues surrounding the use of evidence recovered from encrypted data. It was underlined that forensic personnel did not decrypt cypher text, but identifying encrypted data and establishing authenticity was critical in many cases. Reference was made to the potential uses of forensic digital evidence which were extensive, both in terms of prosecutions and the development of further investigative leads. Different procedures were followed at crime scenes, where the primary objectives were to identify, gather and preserve evidence, and in laboratories, where analysis, authenticity and similar matters were priorities. Regarding the development of appropriate technical assistance and training materials, it was noted that most of the necessary materials already existed in the more general context of cybercrime, and would only need to be modified or supplemented to fit the needs of training those who needed them to deal with electronic forms of identity-related crime.

49. The potential relevance of other, less-direct, types of forensic evidence in identity-related crime cases was examined. It was stressed that, for example, DNA evidence could be used to identify persons who had stolen identity information in a physical burglar. In this connection, the possible nature and range of types of forensic evidence in identity-related crime cases was discussed. The core group was reminded that the basic functions of forensic evidence were usually to establish physical or virtual presence, to establish some form of action, or to establish links between persons, places and/or activities. For example, DNA evidence might also be used to link an individual to a specific computer, digital analysis might then establish the identity of digital documents created or transmitted by that computer, and decryption and/or forensic analysis of those documents might finally be used to establish the criminal nature of the entire process. Generally, based on the views of the experts and the findings of the intergovernmental

expert panel in its 2007 study,¹¹ members of the core group felt that there would be a need for capacity to deal with tangible evidence, such as paper documents, digital data and other intangible evidence, and in cases where information technologies were used to forge paper documents, various combinations of both. It was noted that the concept of “evidence” would be broader than just evidence in the juridical sense. In many cases, evidence gathered and subjected to forensic analysis was more likely to be used to generate leads and further investigations than to play a major part in criminal prosecutions. Other experts noted that evidence based on stored or transmitted data was often so ephemeral that it might only be useful for immediate investigative applications. Differences in the technical ability and legal basis of law enforcement and the private sector for obtaining such evidence were also discussed. While the private sector had greater technical capacity and fewer legal constraints, this made it much more difficult to use any evidence gathered in criminal justice applications. There needed to be both technical and legal standards and practices for the immediate preservation of ephemeral evidence by the private sector pending legal authority to seize or transfer it to law enforcement. There was also discussion of the need for training on how to effectively present the results of such analysis through written reports, graphic and digital aids and other means. Apart from maximizing the effectiveness of the evidence, this was seen as important in routine cases, where documents might be used *in lieu* of *viva voce* testimony, and in transnational cases, where they might aid the courts of one country in understanding and accepting the forensic analyses of another country.

50. One question raised in relation to identity crime cases was how forensic capacity could be used to best support investigators and prosecutors. Another question was related to the need to provide materials not only dealing with forensic analysis, but also with basic investigative capacity to gather and preserve evidence intact for such analysis. Some experts noted that forensic analysis was also often needed to trace or identify victims and other interests affected by a crime in order to minimize harm and support remediation. They also noted that forensics could be used to link digital devices in various locations, and in some cases types such as DNA evidence could be used to link specific persons with devices. There was also discussion on the varying degrees of sophistication required and the corresponding costs. While there were major cases that justified extensive work by highly-trained experts, one expert noted that probably there was a major need for larger volumes of less-sophisticated investigative and other personnel to deal with the volumes of more conventional identity-related crime. Another expert suggested that one possible solution for developing countries might be to be given access to experts and expert facilities in developed countries with both the resources to maintain such capacity and the case-loads to justify it. It was suggested, in this regard, that developing and maintaining a roster of suitable experts and facilities to facilitate such assistance on a case-by-case basis might be a further role for UNODC.

51. Another potential use for forensics, in combination with other investigative and analytical functions, was for pattern-analysis to identify trends in criminal techniques and clusters of occurrences. It was noted that this sort of function required a two-way flow of information. Forensic experts might spot trends or clusters and alert law enforcement agencies, or enforcement agencies might suspect such trends or clusters and seek confirmation by forensic links. This sort of analysis posed additional problems. In order to identify patterns in large volumes of documents or incidents, it was necessary to establish some form of data-base, which, in turn, required some means of standardizing the information entered into the database. It would be necessary to find some way to coordinate the data put into the system for a wide range of different documents and for many different forensic examiners. The system would also require some form of classification of different characteristics used to identify forged or altered documents in order to facilitate analysis. Providing for the input of data and access by forensic and law enforcement experts at a global level would pose a major challenge, but would be essential if the system was intended to deal with transnational identity-related crimes and especially those involving passports or other

¹¹ E/CN.15/2007/8 and /8/Add.1-Add.3.

travel documents. There was some discussion of whether existing software designed for law enforcement or other applications would be adequate for such an application, and whether it could be established and maintained by Interpol. To ensure the accuracy of data in a system, inputs would probably have to be limited to forensic experts, but it was noted that many non-experts would need access to the data in order to identify patterns at the operational level.

52. The question of setting standards for forensic evidence relating to identity crime was also discussed. In general, these would be the established standards for the examination of digital or tangible documents. The role of UNODC in assisting national laboratories to meet accepted international standards was highlighted, together with the advantages of this, including the general reliability of evidence and avoidance of wrongful convictions, as well as the facilitation of effective international cooperation. One expert noted that forensic examiners were something of a scarce resource, and that the establishment of examination standards and the certification of laboratories and experts had led to the use of examiners' certificates or similar processes in which written reports could be submitted as evidence in criminal trials. Other experts noted that this depended on the nature of the evidence and whether the ability to cross-examine the forensic expert was essential. This varied from State to State, but experience with breath analysis for blood-alcohol content and other relatively straightforward and high-volume forensic practices suggested that standard setting and the use of certificate evidence might be a useful element of technical assistance projects. Written forensic evidence might also be useful in cases where evidence was referred to foreign laboratories, although this was less likely in major cases or with very complex analyses.

53. A further issue discussed was the need for general awareness-raising. Many prosecutors, judges and even criminal investigators were not well-informed of what forensic analysis could or could not accomplish. In some cases, under-utilization might result in unsuccessful investigations or prosecutions because important evidence was never recognized or was tainted or contaminated before analysis. In other cases, forensic scientists sometimes faced unrealistic expectations. There was general agreement that part of the process should include efforts and materials directed at line enforcement, administrative and other officials. It should serve to sensitize front-line field staff as to the nature and scope of document abuses and identity crime in general. It should also serve to educate such officials as to the nature and preservation of forensic evidence and the potential importance of such evidence in supporting investigations and prosecutions. One expert indicated positive experiences with such practices/initiatives as "open door" days in laboratories. Another noted that, as with other technical assistance materials, awareness-raising materials would need to be modular and tailored to a range of basic audiences, most of them not very sophisticated in terms of forensic science. Another expert referred to the possible scope of awareness-raising, including educating judges and others about the strengths and weaknesses, possibilities and limitations of forensic analysis evidence, as well as the lengths of time needed in many cases to carry out such analysis. Awareness-raising was also seen as critical to ensuring that adequate resources were allocated to establish and maintain laboratories and train experts. There was general agreement on a need for awareness, but also for the understanding of all concerned of what was necessary to ensure the effective gathering, analysis and use of forensic evidence, and of what was possible if the necessary steps were taken.

54. Discussion was further extended to the nature and types of training that might be needed to enhance forensic capacity to deal with identity-related crime. As with the development of materials, it was apparent that a range of options of varying sophistication would be needed depending on the target audience. There might be some need for fairly basic training in areas such as the nature and use of information technologies, both by offenders and by law enforcement officials. Several experts noted that materials and training possibilities already existed in related areas such as fraud and cybercrime, and that one task for UNODC would be to adapt existing capacity and fill in any gaps in order to deliver training focused on identity-related crime. Such training might be implemented in stand-alone seminars or courses, or integrated into other broader technical assistance and training initiatives in areas such as cybercrime or transnational

organized crime. Identity-related crime forensic elements would also probably be needed with respect to initiatives dealing with other related criminal activities such as money-laundering and trafficking in persons. One expert noted that, as with the supporting materials, it would probably be most efficient to develop training activities first for the most sophisticated audience, and then edit out detailed elements to produce more flexible and compact modules for less-sophisticated target groups and for inclusion as elements of other related training activities. A module training for front-line immigration staff on how to identify falsified passports might be added to courses dealing with trafficking in persons, for example. Another expert noted that, while some materials would focus on the details of forensic analysis, the less-detailed versions would be directed at enabling front-line officials to detect forgeries and to preserve and protect evidence while calling in more specialized investigators and analysts. In many cases, the key problem was not with small numbers of very sophisticated forgeries but with very large numbers of more routine abuses.

55. There was general agreement that training should be formulated so as to support not only investigative needs, but the needs of prevention as well. One expert observed that this would require the capacity for front line staff to spot problems, and for the rapid analysis of documents and dissemination of forensic and other information as intelligence. This would further require two-way communication, as front-line staff was usually the primary source of documents for forensic examination and broad-based information for pattern-analysis, and, at the same time, were also a major target group for forensic information about the latest developments and trends in forged documents to enhance their abilities to identify and act on them. Forensic research was also seen as a key element in the development of new forms of documentation that were more resistant to tampering and which would be easier to identify with only basic equipment if tampered with. It was noted that, in essence, forensic experts often drew attention to reverse-engineer forgeries to determine how existing security measures had been defeated with a view to identifying further forgeries and altering security measures to make further tampering either impossible or more easy to detect. Some of this could be based on the results of actual cases. However, forensic research, in which experts themselves attempt to tamper with documents, was also seen as useful, and as one area where capacity could be enhanced in developed countries with a view to disseminating the results.

56. There was also discussion of the potential roles of the private sector in prevention. These rules were substantial in general,¹² but some specific roles in the context of forensics were also noted. One expert indicated that it was private sector entities which were often in a position to spot crime patterns first and therefore it was important that they be willing and able to alert law enforcement at the national level. Private sector entities were also often responsible for the creation of secure documents and the development of specific elements intended to make them more secure, which required both private research and collaboration with official entities identify and address evolving crime problems. Another expert noted that most of this work should operate through existing entities and relationships as much as possible, and that, as with other elements, preventive information needed to be able to address target audiences at all levels of sophistication. From a standpoint of resources, it was noted that resources for prevention could be sought and justified based on an economic analysis in most countries. Such analysis could demonstrate that using prevention to reduce identity-related crimes was far more cost-effective than reacting to offences with investigations, prosecutions, international cooperation and victim remediation.

57. The core group agreed that there were already relevant materials in existence in many areas, and that the main focus for UNODC should be to compile those materials and modify them as needed for various target audiences, as well as identify and fill in any gaps. The Rapporteur suggested that the primary function for UNODC should be to compile and assess existing materials, reformulate them into terms appropriate for international or global applications, and for the various target audiences to be addressed, and then disseminate and use them for training,

¹² See E/CN.15/2007/8/Add.2, paragraphs 57-60 and E/CN.15/2007/8/Add.3, paragraph 30.

awareness-raising and similar technical assistance applications. Several experts noted that there was a large volume of material in existence, but that it would need to be assessed for validity and quality before any use. Key roles of the UNODC would therefore be to review materials for quality and universality, assemble materials and projects with a range of different national perspectives, as well as develop and use expertise on how to carry out training and other functions on a multilateral basis. In the private sector, much of the existing information and expertise was likely to be found in the area of economic fraud, bankruptcy, and a range of digital and on-line security interests. Both fraud and cybercrime were seen as areas where materials would be easier to locate, and where the main challenges would be to obtain permission to use them and adapt them to projects directed at identity-related crime. Similarly, much of the future work of the UNODC would probably consist of incorporating identity-related crime and economic fraud elements into existing programmes and projects, as opposed to creating dedicated projects.

58. In discussing basic process and time-lines, there was general agreement that UNODC should start with a basic compilation of materials, gathered with the assistance of the experts, where possible. Drafts should then be reviewed by the experts, revised as necessary and then presented to Member States. Pilot projects involving individual States or regional meetings were seen as one way of testing and improving the materials. Another task for UNODC would be to develop a roster of appropriate experts who could assist in training activities. It was underlined that UNODC did not itself have this capacity, and it would be necessary to identify experts from supportive Member States. Some precedents in the area of training on narcotic drugs and psychotropic substances might be followed, but it was noted that past drug-related projects had focused on laboratory capacity, whereas with identity-related crime there was a larger element of field work and the boundary between investigative and forensic elements of the process was far less well-defined. It was also noted that it would be important to have experts from the private sector involved, both in the development of materials and the delivery of training. Aside from basic forensic expertise, there was a need to look at ways to establish and enhance pattern recognition, including standards for reporting and tracking cases, enhanced capacity for information sharing and the development of some form of resource library or database.

59. A brief presentation on the work of the anti-phishing working group (APWG) was also brought to the attention of the core group. This included some forensic work from a different perspective, that of the private sector. The major part of the work of the APWG was a list, updated every 5 minutes, of phishing websites, which could then be used by web-browsers to identify sites and alert users. This work was quickly expanded to fraud, and the lists now included event data using sequences of operations to help identify sites. It had also branched out into text in a number of different languages, enabling web-browsers to identify non-English websites. Aside from blocking sites, the APWG increasingly inserted new links re-directing users immediately to alert them they had visited a phishing site, and to provide educational material about phishing. Other entities, including web-browsers, were also able to automatically redirect communications to this site. Some differences between evidence gathered by APWG and that gathered by law-enforcement were discussed. Generally, APWG's data could be to a lower standard, since criminal evidence and proof were not necessarily requirements. The APWG used the data to screen websites and warn internet users, and law enforcement usually used it to generate other leads or as the basis for more formal investigative measures. This meant that the APWG could move quickly enough to prevent or mitigate criminal consequences, in that ongoing phishing operations could be interrupted. This, however, made it more difficult to interface with criminal justice systems, which moved much more slowly but to a higher standard of proof and with basic human rights safeguards.

IX. Agenda item 11: Mapping out a course of future action for the core group

60. Under this agenda item, the core group summarized all considerations and feedback received with regard to the structure of its future work in the different fields presented above. Emphasis was given to the crystallization of views on the development and use of materials for technical assistance in all of these areas (see under each specific agenda item and the conclusions below).

Annex: Conclusions

1. General conclusions

- The core group welcomed the adoption of ECOSOC resolution 2009/22, which called for the development and delivery of technical assistance on matters relating to economic fraud and identity-related crime.
- Concerning awareness-raising with respect to the work of the core group itself, there was general agreement that the report of the present meeting and the revised documents on criminalization, international cooperation, and if feasible, on forensic matters, should be submitted as Conference Room Papers to the Commission on Crime Prevention and Criminal Justice at its nineteenth session, to be held on 17-21 May 2010.
- Concerning priorities and the sequencing of projects, the core group noted that the secretariat had been directed to report to the twentieth session of the Commission on Crime Prevention and Criminal Justice, in April 2011. In considering the various materials which were being developed, in accordance with the resolution, the core group felt that it would be possible to finalize some elements sooner than others, both as a matter of priority and due to the availability of experts, information and other materials. Generally, the core group concluded that materials on definitional and criminalization issues, as well as international cooperation, inventory of best practices between public and private sector and forensic issues would come first. The next step would be materials dealing with victims, for which further research and discussion with experts on victim issues would be needed. Some of the experts agreed to assist in such research. The materials discussing forensics would also be prepared and disseminated through the Commission. Other materials yet to be identified, would be addressed after that. The core group understood this sequence to be generally in line with the priorities expressed by Member States in formulating ECOSOC resolution 2009/22.
- In dealing with the full range of identity-related crime issues, members of the core group identified a need for the work of UNODC to address offences against both intangible electronic elements of identity and paper-based or other tangible elements. To a certain extent, this might entail the tailoring of materials or projects to suit that nature of national or regional identity infrastructures. However, it was clear that the use of information technologies and other high-technology means by offenders constituted as much of a problem for tangible infrastructures as did more traditional criminal techniques. In that context, materials and projects would need to address all aspects of the problem.
- Cooperation with other relevant organizations at the domestic and international levels was considered essential by the core group. Identity abuses were commonly associated with other forms of crime, such as cybercrime, economic fraud, and money-laundering, and members of the core group felt that there would be substantial synergies to be exploited and it would be necessary to avoid inconsistency and duplication of effort. The core group noted the attendance of the representative from ITU, welcomed the willingness of that Organization to cooperate and support ongoing work and strongly supported the establishment of cooperation relationships between UNODC and ITU through the appointment of liaison contacts and the enhancement of communication channels between the core group, on the one hand, and the ITU-T Study Group on Identity Management, on the other. The core group also considered the feasibility of some collaboration with Interpol and the ICAO in areas such as the setting of technical standards for documents and the compilation of data that could be used for pattern analysis and prevention. However, the group expressed no specific view on the possible modalities of such cooperation or the feasibility of specific projects.

2. Definitions and criminalization

- The core group discussed the question of finding a balance between the need for common approaches to criminalization, in order to support more effective international cooperation, and the need of each Member State to adopt laws consistent with national practice and legislative context. The group understood that such a balance would have to be struck by each Member State, but that technical assistance should be developed with a view to encouraging consistency of approaches and the formulation of similar offences to the greatest extent possible. In general, the group saw the role of UNODC as one of encouraging common approaches to criminalization and finding ways to tailor common offences to the needs of national identity infrastructures without compromising the viability of the offences as a basis for international cooperation.
- Regarding the nature and format of materials to be produced, the core group identified several key issues which would allow such materials to be directed at Member States of different needs and infrastructure:
 - The degree of technological development usually determined the extent to which national identity infrastructures were digital or paper-based, and hence the formulation of some aspects of criminal offences and investigative powers. That said, the core group also referred to the conclusions of the 2007 study to the effect that all Member States were concerned about the use of modern technologies to commit identity related crime, regardless of their approaches to identity infrastructure or degree of technological development.
 - Differences of approach to criminalization, evidence and other matters between common-law and civil law States were also noted in this regard. Members of the core group felt that technical assistance materials needed to be appropriate for each system, while at the same time informing each type of system of the practices and needs of the other in order to facilitate cooperation. It was also concluded that, in general, materials which were based, to the extent possible, on offender behaviours as opposed to legislative responses, would be more useful to both systems, and more likely to encourage common approaches to criminalization.
 - The core group considered the question of whether to criminalize at all identity abuses *per se* as one between civil law States, which preferred legislative restraint and the use of existing preparatory offences, and common law States, which were more inclined to enact new offences. This was also seen as an issue for the Member States themselves, but the core group felt that there were advantages to criminalization, even in civil law States, and that these advantages should be set out in any technical assistance materials.
 - Members of the core group also noted the differences between States with centralized national identity infrastructures and those following a more ad-hoc or subject-specific approach. The group concluded that this affected the formulation of existing offences established to protect identity infrastructures and hence the formulation of entirely new offences that would have to be consistent with what was already in place.
- From a strategic perspective, the core group noted that a key issue in criminalization would be to develop offences broad enough to address the full scope of the problem, while, at the same time, limit their scope to avoid over breadth, legality, human rights and constitutional problems, and also to avoid practical problems with domestic investigations and

international cooperation. The specific means of limiting scope might be, to some extent, different in civil and common law systems, but the basic need to limit scope was common to both systems. There was general agreement that technical assistance materials would need to discuss the basic problem and provide a range of options for both defining conduct to be criminalized and excluding from offences conduct which was innocuous or ill-defined.

- The core group discussed some options for using the many different specific aspects of offences considered to produce general materials. The secretariat may wish to consider, for example, the development of a core list of criteria or issues that would be common to all systems and scenarios and then a series of more specific clusters of criteria linked to the more specific circumstances of the different categories of States and legal systems. There was general agreement that much of the material could and should be based on, or organized according to, offender behaviours. Members of the core group expressed the view that the 2009 G-8 classification,¹³ including the classification of offences based on a chronological sequence of offender acts, would be a good basis for doing this.

3. International cooperation

- Members of the core group noted that in some cases, law enforcement simply saw complex transnational identity crime cases as too complicated to be worth the effort of pursuing. A key element in any international cooperation materials should, therefore, be the availability of basic information to inform law enforcement that effective international cooperation was feasible in identity crime cases and could be made to work at a practical level. The core group felt that one way to accomplish this might be through the use of cases or case-study materials. Therefore it welcomed the use of such materials in the manual on international cooperation which was brought to its attention, as well as the fact that the presentation of those materials illustrated the differences between common law and civil law systems and provided examples of effective cooperation.
- There was also some discussion of the relationship between informal cooperation through the private sector and more formal means through international legal instruments, agreements and arrangements. While there were numerous practical advantages to informal modalities, the core group noted that these raised clear concerns about the possibility of circumventing human rights protections and other legal safeguards, as well as national sovereignty concerns in some circumstances. However, the group also noted that some forms of information did not raise these concerns, and there was general agreement that such types should be identified and that relevant technical assistance materials should encourage informal information-sharing to the extent possible within legal constraints. Joint investigations should also be encouraged.
- International cooperation materials and the delivery of technical assistance should take advantage of synergies, to the extent feasible, with technical assistance under the auspices of the UNTOC. This included both synergies in the development of materials and the delivery of projects. The core group noted that paragraph 9 of ECOSOC resolution 2009/22 called for the transmission of the results of the thematic debate held at the eighteenth session of the Commission on Crime Prevention and Criminal Justice to the Conference of States Parties to the UNTOC. In this connection, there was general agreement that other materials produced following that debate, such as those prepared for the purposes of the work of the core group,

¹³ See E/CN.15/2007/CRP.9.

also be made available to the Conference, and, if appropriate, to its working group on technical assistance matters.

- Given the high probability that many identity-related crimes would involve elements of transnationality, the core group felt that technical assistance materials should provide advice on how to establish rules that would ensure adequate jurisdiction to investigate and prosecute transnational offences, as well as practical advice on how cases involving two or more Member States could be most effectively managed, consistent with customary international law and, where applicable, the UNTOC.

4. The protection and support of victims

- The core group noted the references to victims in ECOSOC resolution 2009/22, including the invitation to Member States to adopt useful practices and efficient mechanisms for supporting and protecting victims of economic fraud and identity-related crime, and the request to UNODC to develop useful practices and guidelines to assist Member States in establishing the impact of such crimes on victims. There was general agreement that a further meeting should be held in late 2010 or early 2011, with the core group supplemented by victim experts, and that the expanded group should be supplied with a document for discussion. This document should contain a summary of the available data and a draft list of best practices for dealing with victims. Invited experts should also be sent a list of questions and asked to bring as much information as possible to the meeting. To the extent feasible, the victim experts should be chosen with regard to equitable geographical representation.
- There was discussion of the need for more information about victim issues, and the difficulty of disseminating further questionnaires. The core group was of the view that sufficient information could be obtained informally. It also recognized that, as it was unlikely that clear and comprehensive information would be obtainable in the foreseeable future, the objective in formulating recommendations for further work in this area would be to provide Member States with an analysis of the strengths and weaknesses of the available evidence and to develop recommendations for their consideration, based on the opinions of the core group, as supplemented by ad hoc victim experts. To support this process, several members of the core group agreed to conduct research in both public- and private-sector resources and provide information or possible sources of information to the secretariat.

5. The development of materials for technical assistance

- There was general agreement that technical assistance materials should be of a modular nature, both in terms of the degree of sophistication and target audiences and in terms of their substantive scope. Generally, it would be advisable to prepare sophisticated materials and then produce less-detailed versions for groups that might not need as much detailed information, and also to produce modules capable of being used in other, larger technical assistance projects, such as those aimed at implementation of the UNTOC.
- As noted, the core group felt that such technical assistance materials should be placed before the next session of the Conference of States Parties to the UNTOC in October 2010.

6. Issues relating to forensics

- There was general agreement that technical assistance materials were needed for building forensic science capacity to deal with identity-related crime. Generally, these would overlap with materials for the examination of tangible, paper-based documents and for digital documents and evidence. Materials for dealing with identity-related crime should draw on

existing materials in these and other related areas, with added content to supplement them and fill in gaps as needed. As with other technical assistance materials, the core group also felt that these needed to be modular, so as to be used alone or as part of more broadly-based technical assistance, and tailored to target audiences of varying degrees of knowledge or sophistication.

- There was also general agreement on the need for training using such materials. This may need to be more broadly-based than the documents, depending on the existing capacity of each State to deal with the examination of tangible and digital documents in general.
- Both materials and training may need to be addressed to a range or continuum of levels. These would include: expert forensic scientists, specialized or expert investigators, general investigators and line enforcement and administrative officials, such as police officers and immigration officials checking passports. Some materials may also need to be directed at judges and prosecutors.
- The core group also agreed that, due in large measure to the increasing role of information technologies, both in identity infrastructures and identity-related crime, this area was prone to very rapid evolution of criminal methods for document tampering and similar activities, and that this made essential some means and process for the regular updating of technical assistance and similar materials.
- There was also general agreement on the need for more general awareness-raising to educate the criminal justice community on the possibilities and limitations of forensic evidence, and how to use it in identity-related crime cases.
- In general, members of the Group identified a need for the transfer of information in both directions. Information from forensic experts needed to flow to those who design and produce documents and to those who investigate criminal offences, to support both prevention and investigation. The flow of information from other officials to forensic experts was needed to provide non-forensic context in criminal investigations, and to ensure that scientific experts were kept aware of new developments in crime.
- There was discussion of the potential uses of a data-base that would give law enforcement officials and forensic examiners access to sample genuine documents for comparison, and also compile information about forged and other illicit documents so as to permit pattern analysis of identity-related crime offences and offenders. Members of the core group noted that establishing such a database would be difficult, especially at the international level, and might be beyond the crime-control mandates of UNODC and the Commission on Crime Prevention and Criminal Justice. There were also potential problems in ensuring consistency of data put into the system in such a way as to permit comparison and analysis. Nevertheless, the core group noted some existing projects of this nature and felt that the idea could be explored further with other organizations such as Interpol.
- The experts discussed the fact that many developing countries would have only occasional need of highly-sophisticated forensic capacity and would not find developing and maintaining such capacity to be cost-effective. In such cases, it might be preferable to have the necessary analysis done in developed countries, which had the resources to maintain such capacity and the case-loads to justify it. The experts noted that one possible role for the UNODC might be to maintain a roster of experts and facilities which could be made available for sophisticated forms of forensic analysis on a case-by-case basis.