UNODC
United Nations Office on Drugs and Crime

Fifth meeting of the Core Group of Experts on Identity-Related Crime (Vienna, Austria, 6-8 December 2010)

I. Opening of the meeting and adoption of the agenda

1. The fifth meeting of the core group was convened by the Chairman, Ambassador Eugenio Curia, representative of the Government of Argentina in Vienna, from 6 to 8 December 2010. In accordance with past practice, the composition of the group featured a multi-stakeholder approach and, in addition to the Chairman, the following experts attended:

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; *Jan Vancoille*, Jurist, General Institutions and Population Home Office, Belgium; and *Edwin Delwel*, Police Commissioner, Programme Manager ID Issues, Dutch Police, Netherlands.
b. Private sector:
Anko Blokzijl, Safran Morpho, Sagem Identification, Netherlands; *Fons Knopjes*, ID Management Centre, Netherlands; and *Pat Cain*, Resident Research Fellow, Anti-Phishing Working Group (APWG);
c. International organizations:
Luca Castellani, Programme Officer, Office of Legal Affairs, International Trade Law Division, UNCITRAL Secretariat; *Jeppe Holt Jensen*, Delegation of the European Union to the International Organizations in Vienna.
d. Academia/individual experts:
Gilberto Martins de Almeida, MARTINS DE ALMEIDA Advogados, Brazil; *Michael Murungi*, Editor/CEO, National Council for Law Reporting, Kenya Law Reports, Nairobi, Kenya; *Marcos Salt*, Professor of Criminal Law, University of Buenos Aires, Argentina; *Eileen Skinnider*, Director, Human Rights and Research International Centre for Criminal Law Reform and Criminal Justice Policy, Canada; and *Baosheng Zhang*, Vice President, China University of Political Science and Law, China.
e. Secretariat: *Demostenes Chryssikos*, Crime Prevention and Criminal Justice Officer, UNODC/DTA/CEB; *Dildora Djuraeva*, Contractor, UNODC/DTA/CEB.

2. 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 3: Review of progress, developments and follow-up activities

3. The Chairman commenced by reviewing developments since the previous meeting of the core group. The Chairman also summarized relevant developments at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Salvador, Brazil, in April 2010, and the subsequent nineteenth session of the Commission on Crime Prevention and Criminal Justice,

and noted in particular paragraph 15 of the Salvador Declaration[1], which dealt with economic fraud and identity-related crime. He noted that paragraph 15 had called, *inter alia*, Member States to continue to support the ongoing work of the UNODC in this area, and enhance international cooperation, including through the exchange of relevant information and best practices, as well as through technical and legal assistance. Furthermore, and in the context of the Congress deliberations, it had been recommended that UNODC continue to cooperate with other intergovernmental organizations such as those which had contributed experts to the Group. [2]

4. The Chairman also reviewed the deliberations of the Congress and the nineteenth session of the Commission on Crime Prevention and Criminal Justice on the subject-matter of cybercrime. He summarized the views of various States about the seriousness of the problem and the need for effective responses at the domestic and international level, ranging from domestic legislation and training to technical assistance and the possible development of a global legal instrument or other legal responses at the international level. He noted that, based on the deliberations of the Congress, [3] the Commission had transmitted a resolution to the General Assembly calling for an open-ended intergovernmental expert group (hereinafter "expert group on cybercrime") to be convened for the purpose of conducting a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. [4] It was noted that the first meeting of the expert group on cybercrime would be held on 17-21 January 2011, and was expected to consider, *inter alia*, methodological options and the availability of data sources for the purposes of the study. Given the relevance of elements of the 2007 United Nations study on "Fraud and the criminal misuse and falsification of identity"[5] and the subsequent work of the core group in this area, the Chairman noted that there would be a need to find ways to integrate the work of this core group with the work of new expert group on cybercrime, which would be to a large extent overlapping, as economic frauds and other identity-related crimes could also be forms of computer-related crime.

5. The core group discussed, in this connection, methodological issues and lessons learned in the course of developing the 2007 study, as well as the subsequent work of the core group, which might prove useful in the new cybercrime process. It was noted that a critical issue in the earlier study had been the establishment of cooperative relationships with other United Nations and other intergovernmental entities to obtain the best possible information, as well as to ensure consistency and avoid unnecessary duplication of effort, as well as to reach out to academic and private sector

---

[1] See General Assembly resolution 65/230 of 21 December 2010, annex. The text of the Declaration is available online at http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

[2] The question of collaboration with other intergovernmental and international organizations relevant to the work of the core group was considered at its first meeting. For a list of the organizations suggested by members of the group, see the Report of the group at its first meeting, E/CN.15/2009/CRP.10, paragraph 23.

[3] A/CONF/213/17, paragraphs 191-208, available on-line at: http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress-documents.html. See also the Salvador Declaration, endorsed by the General Assembly (see GA resolution 65/230 of 21 December 2010, annex).

[4] E/RES/2010/18, paragraphs 9 and 11, available on-line at http://www.un.org/en/ecosoc/docs/2010/res%202010-18.pdf. Subsequently adopted as A/RES/65/230.

[5] See E/CN.15/2007/8 and Add.1-3.

interests to ensure that their expertise and views were taken into consideration, both directly and through the involvement of UNCITRAL. In this context, several experts noted that one of the reasons for the establishment of the core group as a non-intergovernmental process was the need to engage academic and private sector expertise in areas where their knowledge was critical to developing viable technical assistance materials and their cooperation would be helpful in the delivery of such assistance, especially in areas such as crime prevention and cooperation with law enforcement. In general, given the nature of cybercrime and the environment in which it is committed, the experts felt that similar access to, and involvement of, non-governmental sources would be useful in the forthcoming cybercrime process, and it was hoped that the core group model might serve as a precedent and an example of the utility of such cooperative engagement.

6. There was general agreement that the cybercrime expert group should be made aware of the work already done in the field of identity-related crime and provided with access to the various documents containing the 2007 study and subsequent work of the core group, with a view to maximizing the value of available resources and avoiding any unnecessary duplication of work. In later discussion, it was decided to transmit a brief overview of the work of the core group to the new expert group. It was also noted that several members of the core group were expected to be involved in both processes and therefore in a position to keep each process advised of the activities of the other.

7. The Chairman also drew attention to the adoption of resolution 19/1 on "Strengthening public-private partnerships to counter crime in all its forms and manifestations" by the Commission on Crime Prevention and Criminal Justice and ECOSOC, which called for greater cooperation between the public and private sectors, and noted the significance of this resolution, both for the ongoing work of the core group and in the context of the forthcoming cybercrime study. He further stressed that the successful engagement of the private sector in the core group process could serve as a useful precedent for the cybercrime process as well.

8. The Chairman also reviewed the mandates of the core group itself, noting that these were subordinate to those established by Member States for UNODC, and that its function is to support UNODC in fulfilling its own mandates. He briefly reviewed the elements of the mandates set out in ECOSOC resolutions 2004/26, 2007/20 and 2009/22, the latter addressing the work of the core group directly. He also reminded the core group that the focus of the fifth meeting on victim issues was as a result of previous discussions and a decision to that effect at the fourth meeting of the group had been made. He then reviewed other elements of the provisional agenda, noting that the present meeting should provide an opportunity to review developments in some of the regions, including Latin America, China and Africa.

9. The rapporteur of the core group reviewed developments in the Commission on Crime Prevention and Criminal Justice and outlined recent developments in Canada. He indicated that Canada's new legislation criminalizing identity theft, which defines "identity information", modernizes identity-fraud and establishes new offences of identity-theft and trafficking in identity information (Bill S-4) had come into force on 22 October 2009. He also noted that further amendments which implement recommendations from the study on "Fraud and the criminal misuse and falsification of identity", by establishing harsher sentences for frauds with aggravating circumstances, were presently before Canada's Parliament.[6] It was also noted that the

[6] Bill C-21 of the 40th Parliament, 3rd Session, First Reading May 3 2010, available on-line in English and French at: http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4488626&Language=e&Mode=1&File=24.

Royal Canadian Mounted Police, in conjunction with other law enforcement and governmental bodies, was in the process of developing a national strategy for dealing with the process developing a national strategy for dealing with identity-related crime, and that Canada's Policy Centre for Victim Issues was undertaking research to assess the nature, numbers and needs of victims of identity-related crime in Canada.

10. The UNCITRAL representative summarized recent work of the UNCITRAL Working Group on Electronic Commerce in the areas of commercial fraud and electronic commerce. He noted that there would be an UNCITRAL colloquium in New York from 14-16 February 2011, which would address questions of identity-management as one of its themes,[7] and there was discussion of whether the core group could transmit a message to the Colloquium regarding its work.

11. Mr. Martins de Almeida briefed the core group on the status of the work commissioned by UNODC on the ddevelopment of a compendium of examples of relevant legislation on identity-related crime (and fraudulent practices linked to it), in line with a relevant mandate of the core group. He noted that, from the outset, identity crime and identity-related crime offences had been difficult to identify and characterize. Most States still had no specific offences established to respond to identity-crime, although a few had started when the core group was convened and more had started work in this area since then. Most States had a number of identity-related crime offences, and here the problem was more one of assessing the wide range of different offences, how each offence addressed the problem and considering whether any gaps existed, given the evolution of criminal techniques. It was underlined that the purpose of the mandated compendium was to take stock of examples of national laws covering the range of possibilities and responses taken by various legal systems. It was therefore not seen as necessary to compile every single legislative provision. As with other aspects of the work of the core group, one problem encountered was the difficulty in assembling legislative provisions from developing States, and Mr. Martins de Almeida reported some progress in this regard. At the time he updated the materials for the present meeting, the compilation had sample offences representing the laws of more than 90 Member States whose legislation had been reviewed. Given that many Member States now post their laws on-line, a list of appropriate on-line location and citation information is being included to assist legislators in finding examples of what other States have done.

12. In discussion, it was noted that the compilation was a supplement to the earlier work that had been done in respect of typology, definitions and possible approaches to criminalization of identity-related crime. In this context, reference was made again to the work of experts from the G-8 Lyon Group,[8] which, in addition to examining the state of the problem and responses to it in G8 Member States, had also proposed a typology of identity crime offences. Reference was also made to similar research work mandated by UNOCD, in line with recommendations of the core group, on the typology and criminalization issues emerging in the field of identity-related crime[9]

---

[7] UNCITRAL Colloquium on Electronic Commerce, New York, 14-16 February 2011. The first session of the Colloquium will deal with the subject matter of "identity management. See: http://www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html

[8] Work of the Criminal and Legal Affairs Subgroup (CLASG), which was presented to the Core Group at its third session and to the Commission on Crime Prevention and Criminal Justice at its eighteenth session. See E/CN.15/2009/CRP.9.

[9] See E/CN.15/2009/CRP.13.

13. In the subsequent work of Mr. Martins de Almeida, several of the bases into which the typology was divided were considered in more detail and in the context of a broader range of Member States, whose legislation has since been reviewed. The majority of offences reviewed and compiled still fell into a broad range of identity-related crimes, including those focused on specific identity abuses or circumstances, such as document forgery, passport abuses or impersonation offences. The offences could be classified in a number of ways, and those considered in the typology compendium included: the different conceptual approaches of civil-law and common-law States; offences based on process or offender conduct and offences based on results or effects; and how inchoate conduct was dealt with. There was also discussion of the overall problems faced by legislators in finding enough breadth to capture the illicit and harmful conduct involved without being so broad as to be difficult to enforce and raising constitutional problems with respect to legality (civil law States) or over breadth (common-law States). There was also some discussion of how some of the types of offences compiled would apply in transnational scenarios, and of the need for an assessment of jurisdictional considerations in this regard.

14. In discussion, it was noted that, once the initial compilation is finished, further work would still be needed on an ongoing basis to keep the compendium up to date, especially with respect to legislation dealing specifically with identity crime, which a number of States are either considering or are in the process of developing and adopting. The possibility of a further questionnaire or the inclusion of relevant questions in other research efforts, including the forthcoming global study on cybercrime, was discussed. It was noted that, on one hand, up to date information was particularly important in a new and emerging area such as identity-related crime, but, on the other hand, "questionnaire fatigue" tended to reduce the willingness of Member States to provide the information.

III. Agenda item 4: Comparative approaches (European Union, Africa, China, Latin America)

15. For the European region, Mr. Vancoillie reviewed recent developments in the European Union. Reference was made to the Stockholm Programme adopted by the European Council in December 2009, which set priorities for developing the European area of freedom, security and justice in the period 2010-2014. One of the initiatives under the Programme is criminalizing identity theft and setting a European strategy on identity management. According to the Action Plan Implementing the Stockholm Programme,[10] the strategy includes legislative proposals on criminalization of identity theft and on electronic identity (eID) and secure authentication systems by 2012. Useful feedback is to be provided by a comparative study on identity management had been carried out and finalized as a follow-up to the Tomar conference (7-9 November 2007) during the Portuguese presidency, on the basis of the replies to a questionnaire by the ID Management Centre in the Netherlands. Another comparative study is currently under way on the best ways to prevent and fight identity theft in the EU Member States. Another The Council of the European Union adopted on 2-3 December 2010 conclusions on preventing and combating identity-related crimes and on identity management, including the establishment and development of permanent structured cooperation between the Member States of the European Union,[11] which referred, inter alia, to the work of the Commission on Crime Prevention and Criminal Justice and

[10] European Commission, COM (2010) 171 final, 20.4.2010.

[11] See *Justice and Home Affairs Committee*, 3051st meeting, 2-3 December 2010, available on-line at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/118173.pdf.

the core group, as well as the United Nations Convention against Transnational Organized Crime and its Protocols against trafficking in persons and the smuggling of migrants, where applicable. In those conclusions, the Council called on the European Commission, among others, to: support Member States' efforts to reinforce personal identification procedures within the EU by taking note of the findings of the Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis carried out in several Member States; support cooperation between Member States by setting up a platform for the exchange of good practices in the area of managing the personal identity chain as a whole and, in due course, a European network of experts; support the establishment of effective complaint mechanisms in the Member States that could provide adequate help to victims, and analyze how to ensure optimal cross-border cooperation between these mechanisms; and support Member States' initiatives on preventing and combating identity-related crimes in the identity chain as a whole, which may include combating these crimes in the criminal justice chain, immigration chain and private sector. Mr. Vancoillie further referred to the conference organized under the Belgian presidency on 27-28 May 2010 on "Identity fraud", which was attended by several experts in this field, particularly in the financial world and in cyberspace.

16. In discussion, it was noted that the conclusions of the Council constituted only non-binding recommendations to the Commission, which, having only been transmitted in December 2010, were still under consideration. It was, however, seen as likely that the Commission would accept and act upon the recommendations. The Council had noted that the development of terminology by the UN process had made it unnecessary for them to define or redefine terms, no European States having thus far needed to define similar terms for legislative or other purposes. The Chairman suggested that a representative from the Council be invited to participate in a future meeting of the core group to inform it of the ongoing European Union work.

17. Regarding the African region, it was noted that a West African Cybercrime Summit focusing specifically on advance fee fraud was held in Abuja, Nigeria, from 30 November to 2 December 2010. Mr. Rusch described the background of the meeting. The Summit was hosted by the Economic and Financial Crimes Commission (EFCC) in collaboration with the United Nations Office on Drugs and Crime (UNODC), the Economic Community of West African States (ECOWAS) and Microsoft. The work of the Nigerian Economic Crime Commission, which deals not only with fraud but also with money laundering and other economic offences, focused on addressing problems which have caused the region substantial harm in economic and reputational terms. The Commission has been examining laws and other measures which exist in West African States, with a view to developing proposed reforms. UNODC and other international organizations have now joined in this effort. One major goal is to develop robust public-private partnerships, including timely information sharing, and Microsoft has also been contributing to the effort. A recent regional "cybercrime" conference had in actual fact focused on electronic and digital versions of fraud and identity crime, starting with initial efforts to prevent and suppress frauds and, it was hoped, future work on identity crime and identity-related crimes in addition to frauds. Mr. Rusch also noted other regional developments, including the recent expansion of the Ghanaian anti-fraud unit, which was originally established to deal only with frauds against the Government of Ghana, to now address all forms of fraud regardless of perpetrator or victim.

18. Mr. Murungi discussed the perspective of the National Council for Law Reporting of Kenya, which reports common law jurisprudence and tracks legal developments. His remarks were focused on the legal environment and framework for the East African Community (EAC) region. His information to-date reflects state of knowledge and the EAC awareness that identity abuse is a crime problem, but more data are clearly needed to put a face on the problem and

objectively assess its nature, scope and the harm it causes. The five States in the EAC[12] are presently engaged in developing a common economic market, as well as a customs and monetary union. With a collective population of about 125 million, this clearly offers economies of scale, but also could generate substantial challenges from the standpoint of identity management and the prevention and suppression of identity-related crime. A further challenge will be the fact that the EAC sub-region is divided between former Belgian colonies (Burundi and Rwanda), which employ civil law systems, and former British colonies (Kenya, Tanzania, and Uganda), which have common-law systems. As is the general practice in developing countries, most of the identity infrastructure remains based on paper documents, and most of the identity crimes of concern are those which target such documents.[13]

19. Mr. Murungi reviewed the range of purpose-specific identification used in the various States of the region. Internet access in the region remains limited, but as with most developing regions of the world, mobile telephone infrastructure has been taken up quickly and is widely available. Offenders have learned to exploit the available technologies and the use of mobile telephones in fraud and other forms of economic crime has become a particular problem as it has become possible to carry out funds-transfers by mobile telephone. A number of identity-related crimes are considered a problem in the region, most commonly in the context of economic frauds and various forms of money-laundering. Among regional governments, there is general support for identity crime legislation, but no uniform EAC provisions have been finalized thus far. Some regional States are Parties to the UNTOC and the UNCAC, but none has yet ratified, or acceded to, the Council of Europe Convention on Cybercrime. The prevailing political view in the EAC is that it would be more appropriate to develop an instrument of their own than to accede *ex post facto* to a European instrument. Other recent regional legal developments were also raised. Most States still retain their original post-colonial constitutions, although Kenya recently adopted a new one. Privacy rights tend to be expressed, if at all, in the form of broad constitutional norms and not in the form of express or explicit statutory rights. This has been done mostly by evolution of the common law in each of the three individual EAC common law States. The exception to this is Kenya, whose new constitution does guarantee privacy rights. The position of civil law EAC Member States could not be ascertained in time for the present meeting of the core group.

20. While there are no express identity-crime offences as yet, identity-related crime is partly covered by conventional criminal law in various EAC States in much the same way as has been seen in other regions. Mr. Murungi indicated that most States in the sub-region had criminal laws dealing with conduct such as fraud, impersonation, and forgery based on the original UK common law or Belgian civil law inherited in the colonial period. The EAC has developed new cyber-law framework as an aid to States developing new legislation regulating technologies and combating criminal misuses thereof. The framework recommends, *inter alia*, that distinct statutes and provisions should be enacted for cybercrime. It also contains principles on data-protection, based on the UNCITRAL model law and other cybercrime precedents, and electronic commerce elements based on UNCITRAL and UNCTAD work dealing with electronic transactions, privacy,

[12] Burundi, Kenya, Rwanda, Tanzania, and Uganda.

[13] This is consistent with the evidence reported to the intergovernmental expert group that produced the 2007 United Nations study. Generally, all Member States indicated problems or concerns about links between information and communications technologies and the economic fraud and identity-related crimes, but whereas developed countries tended to be concerned about conduct such as on-line "hacking", theft of and trafficking in digital identity information, developing countries were more concerned about the use of computers and sophisticated printers to produce high quality forgeries of identity documents and documents used in various frauds. See E/CN.15/2007/8/Add.2, paragraph 26 and E/CN.15/2007/8/Add.3, paragraph 24.

data-protection standards and similar matters. There is general support in the region for implementing the framework and Mr. Murungi reviewed the progress of States at various stages of implementation. In Kenya, the national telecommunications statute has had regulatory powers for some time, but these had not been used to set standards until fairly recently. After a series of 2009 law amendments, new provisions were added on cybercrime, dealing with matters such as unauthorized access to computer systems or data, and accessing computer systems with intent to commit offences. Also included were offences in relation to passwords, mobile telephone misuse, electronic fraud offences, and consumer protection measures to protect the security of data, including personal information.

21. Many new types of criminal offence have appeared in the EAC sub-region, raising concerns about the need for legislative and other responses. Some of the new offences encountered were linked to the dominant technology – mobile telephones – which have been linked to an increase in kidnapping by creating a secure and untraceable means for offenders to communicate with victims. Access to mobile telephones by members of organized criminal groups in prisons, which are used to continue criminal operations, is also a serious problem. As in other regions, the legal and practical constraints and implications of cooperation between law enforcement and communications service providers is also an issue, both in terms of the extent to which information or content may be disclosed to law enforcement and of whether they can deny service to known or suspected offenders and if so on what legal basis. Lack of coherent statistics is also seen as a problem. A range of different law enforcement and other entities deal with cases, and many cases are dealt with by magistrates or lower courts where they do not generate formal reports. Regarding victims, there is no conceptual framework on identity crime, which means law enforcement and other personnel receive no specialized training. The legal framework was also seen as inadequate, with most of the focus directed towards retributive measures and not prevention or other harm-reduction policies. The lack of access to effective legal aid is a widespread rule of law problem for most of the African region, and this extends to victims of identity related crime as well. Some cases have transnational aspects, and the lack of international cooperation poses a problem when they occur. States sometimes find it necessary to discontinue cases due to evidentiary or cost obstacles. There is a need for the study of identity and identity-related crimes in the region, and for efforts to compile and assess such data as presently exists, from both law enforcement and private sector sources. This is both a research issue and one which raises more fundamental issues about how information is accumulated in the first place. In general, the EAC sub-region has needs which are consistent with those identified more broadly by the 2007 United Nations study.

22. In discussion, the Chairman noted that the EAC sub-region faces many of the same challenges as other regions – how to define and identify victims, and how to persuade diverse sources of data to cooperate in sharing it. It was necessary to gather data from all possible sources and perspectives, including data from the private sector and from victims. Other experts noted that the role of mobile devices is critical in developing countries, where the uneven distribution of devices and supporting technologies, such as SMS text messaging, remains a problem and an influence on crime patterns. Simpler versions of technologies tended to pose more serious challenges with respect to identification, and hence proportionally greater opportunities for criminal offenders. It was also important to highlight that the basic types of criminal offence tended to be the same everywhere, only modified to suit the opportunities and constraints of the various technical environments in which they were committed. It was further highlighted that the region would also face the challenge of seeking a reconciled and coordinated strategy between the sub-region's civil and common law Member States in what the 2007 United Nations study refers to as "common approaches to criminalization". A question raised was how a wider array of experts from the region could be identified and engaged in the ongoing international work. In this

subject area, it is often difficult to find a starting point from which to work outward with legislation, training, and other measures. Mr. Murungi replied that, in Kenya, several civil society entities had become active on information technology and cybercrime issues, as well as with victims. They appear presently to be looking at victim issues as part of broader package of consumer protection issues, but it was felt that this could provide a useful starting point.

23. Mr. Zhang delivered a presentation on identity crime issues in China. The country has a centralized national identity system, with some use of digital technologies, but relying primarily on paper documents. Regarding legislation, two recent trends could be observed. China has always taken measures against seriously malfeasance by public officials and a series of identity-related criminal offences relating to the misuse of identity information or documents by officials have been in place for some time. Apart from this, until recently much of the focus for dealing with identity abuses has been on tort and other civil recourse by victims themselves. This has recently changed as the coverage of the criminal law has expanded from identity abuses by public officials to identity abuses by anyone, and as the overall focus of the law has shifted from private civil recourse to State-based prosecutions and criminal sanctions. A major shift took place with the enactment of the first identity-crime amendments in 2009. These included offences dealing with matters such as the forgery of identity documents, identity theft, unlawful possession of identity documents and unauthorized collection of identity documents. Further changes to modernize the law are continuing. As with other Member States, China has also had for some time a number of offences which dealt indirectly with identity-related crime problems, such as offences dealing with forgery, money-laundering, frauds and counterfeiting of trademarks. The recent series of amendments has also included non-criminal elements strengthening elements of the identity infrastructure itself. Future changes to the law in China are likely to include legislation establishing an "identity theft" and crime translated as "cheating and bluffing", which is likely to be similar to impersonation and identity-fraud, but possibly broader in scope. Some attention is also now directed at prevention and the protection of victims. The Chinese Academy of Social Sciences recently began to look into personal data protection issues, and this has led to the adoption of an extensive Personal Data Protection Act.

24. Mr. Zhang also described several cases illustrating the old and new approaches to identity-related crime. As in other States, identity crime and fraud schemes that systematically target victims have been encountered and there has been a series of recent prosecutions in which multiple frauds and/or victims were involved. In 2009, the Chinese Supreme Procurator supplemented the law amendments of that year with regulations which established aggravating circumstances for some offences, such as tampering with large numbers (more than 10) of credit cards, and in one case mentioned this had led to a sentence of 8.5 years. China has also continued its vigilance with respect to identity abuses by public officials. One of the 2009 amendments added a new provision to the law criminalizing abuses of official position to obtain or misuse official identity documents for transport, medical treatment or other advantage, and another offence deals with circumstances where an official takes and sells another's identity. The Supreme Procurator has also interpreted the 2009 legislation as extending to cases of trafficking in identity information or documents, and the Chinese Supreme Court has upheld these interpretations. One recent trafficking case had led to a one-year prison term and a substantial fine. There have been many of the same scope and definitional issues seen in other States, and China's courts have on occasion addressed interpretive ambiguities in the legislation, but on the whole, a sufficient degree of deterrence appears to have been achieved.

25. One current scope issue has been whether some the older offences which have until now applied only to malfeasance of public officials should now be extended to abuses by private citizens in response to new offending patterns and opportunities provided by access to

technologies. Another issue is that many of the existing offences criminalize related conduct using invalid or illicitly-obtained identification, but not the stage of illicitly obtaining it in the first place. A further issue was the quantification of harm for purposes of sentencing. While law amendments have clarified the issues to some degree, quantifying harm arising from identity-related crime offences such as economic fraud is generally much easier than establishing the seriousness of the crime and the harm caused when identity crimes were committed but there was no subsequent misuse of the identity or where the criminal scheme was disrupted by the intervention of law enforcement at that point. As in other States, thus far, most judges in China tend to treat identity crimes as an adjunct to the related conventional crimes rather than as separate and distinct offences, where the factual situation will support this, because it is easier to do so. As reported by many Member States in the 2007 United Nations study, identity-related elements have also been encountered in a wide range of other criminal offences in China, both as part of the offence itself, such as the use of impersonation and false documents to fake kidnappings to extort money, and as a means of avoiding detection, prosecution and punishment.

26. In discussion, it was noted that China also faces similar problems encountered in other Member States with respect to the gathering and analysis of crime statistics in this area, in that statistics are not always collected, and when they are collected, there tend to be multiple overlapping offences, and as noted, judges have a tendency to classify offences with identity-abuse elements as more conventional crimes where the facts support such a course of action. It was also noted that China sees similar relationships between the spread of technologies and identity-related crimes in the sense that offenders tend to adapt and exploit whatever technologies are locally available and give them access to victims and/or funds. Generally, identity-related crime is more common and a more serious problem in the major cities, where opportunities for offenders are greater. Another challenge for Chinese law-makers was the question of dealing with identity information which was legally-obtained and then misused either to commit identity-related crimes or to gradually accumulate a comprehensive identity by using “breeder” documents and processes as the basis for deceiving more rigorous and secure identity-issuance processes.

27. Mr. Salt discussed the results of his research concerning developments in identity-related crime and State responses to it in the Latin American region. He noted that, as with other regions, identity-related crime is not new in Latin America. Almost every national criminal code has relevant offences, and ongoing and further developments were more a question of modernising and updating what already existed than of creating entirely new law. Not much specific research has been done, and national statistics tended to be limited to the more serious forms of crime in general. Data on economic crime was harder to obtain, partly because it was not gathered, and partly due to the overlap between identity crime and other economic crime offences. This made it necessary to start research into the issue more or less from first principles. While the basic nature of the crimes has not changed, what has changed recently in the region is the globalization of such crime and the involvement of organised criminal groups operating on a transnational basis. One scenario given as an example was the use of the boundary region between Paraguay, Argentina and Brazil, where law enforcement is weak. This area has become a source of false documents and fabricated identities, many of which were then used to migrate north. The comprehensive nature of many of these the false identities made it difficult to detect the forgeries. A further form of identity crime encountered in the region was the use of false identities to vote in elections. Mr. Salt reported that in some Member States, temporary increases in fraud and similar crimes had been noted, in post-election periods, as false identities created in order to vote illegally were then sold and/or put to other uses by criminal offenders. More generally, various forms of fraud were probably the crimes most commonly associated with identity crimes, and these included specific forms of tax fraud and tax evasion.

28. Changing crime patterns in the Latin American region suggested that identity fraud crimes were increasing as increasing reliance was placed on digital identification and the use of data bases, many of which lack adequate security measures. There is also a lack of centralization and cross-checking when verifying identity, which allows crimes to continue. Often victims remain unaware that there were problems for extended periods. While technological changes are seen as driving some expansion and changes in identity-related crime, more traditional forms of crime remain a major problem because paper identity documents are still in widespread use. Whether electronic or traditional means are used by offenders, the impact of identity-related crime is now seen as transnational. In cases of ATM card fraud and credit card fraud, for example, either elements of the crime or its effects usually affect companies and individual victims in more than one place. Forms of cybercrime related to identity are also becoming a serious concern in the region. The infection of computers with BotNet and other hostile software is widespread and a serious problem. Such software was used to steal identity and other information, directly for fraud and phishing and in the case of BotNets, to obtain identity information, bank-access information and similar data. Trafficking in identity information into, out of and within the region is also an increasing problem, both for law enforcement and for legislative bodies. In some States, identity information is not yet covered by existing theft or cybercrime offences and trafficking or selling such information is not a crime.

29. Mr. Salt indicated that some law reform was needed to support international cooperation, but in most States the basic criminal offences to support already existed. Most of the gaps involve the fact that trafficking scenarios are not addressed. Theft and trafficking may not apply to data because it is not "property", for example. As in other regions where civil law systems predominate, the question of how far criminal liability should be extended back into preparatory conduct for related crimes such as fraud varied from State to State. Most of Latin America tends to follow German law, which does not criminalize preparatory conduct, and the question of whether some identity abuses should or could be criminalized independently based on direct harm to victims was discussed. On one hand, it could be argued (as the core group has maintained) that conduct such as the taking and trafficking in identity information cause independent harm even if no other offences are committed and should therefore be criminalised separately. On the other hand, experts with civil law backgrounds noted that the legality principle limits what can be criminalized where there is no direct link to the causation of harm, and that this might be difficult to establish in scenarios where a person's identity information was taken and nothing further was done with it, even if it had been sold on to traffickers. It was noted that some of those concerns might be addressed by having concise and clear definition of the proposed offence. This could be difficult to formulate, but would help establish the underlying need to base offences on essential interests that need to be protected. In this case, the policy basis of such offences is the need to protect the integrity of the identity infrastructure.

30. Concerning cybercrime offences, examples of new or pending legislation on phishing and pharming from Colombia and Costa Rica were also highlighted by Mr. Salt and discussed. Gaps in the laws of some Latin American States permit hosting of trafficking sites in the region, which is becoming an international problem. In Brazil, data-protection laws are being used to suppress such activities, but these are not as effective as the criminal law. Messrs. Salt and Martins de Almeida both highlighted the difficulty faced by States in this region in developing new crimes dealing with trafficking in identity information. Even where identity information is designated as quasi-property and/or a commodity that can be trafficked, it is difficult to criminalize trafficking in isolation, and it is also not automatically linked to anti-organized crime legislation. Mr. Martins de Almeida noted that offences of trafficking in identity information were presently being prepared in Brazil, both as independent offences and as an aggravating factor for electronic

forgery. Several States have or are preparing offences dealing with computer fraud. This was not seen as a major departure from existing fraud offences, just a question of adjustment.

31. With respect to other legislative developments, and best practices, criminal procedure reforms have also been made or are underway in some States, including transformation from inquisitorial to accusatorial systems. Evidence laws suffice for ordinary investigations and prosecutions, but there is a need for modernization in most States to deal with electronic and digital evidence issues. Some States have begun to establish databases for stolen identity information or documents. Chile, for example, encourages reporting and once the theft is reported, is made accessible to banks and other users and limits any further liability of the victim. In some States basic infrastructure changes are underway that will prevent crime and support criminalization though the use of biometric and other technological enhancements. This causes general identity-management issues in the sense that reforms must be comprehensive to work, and this can be a problem, especially in regions where the underlying technological infrastructure is not there. In the region, this can often be an urban-rural difference, which makes it more difficult to implement comprehensive national identity infrastructures without weak points resulting from uneven technological implementation. Incomplete implementation can be dangerous in the sense that if technical data are gathered and not well protected, the risk of harm increases because users place too much reliance in systems that still have weak points open to attack by offenders. Specialist police units dealing with cybercrime (through Interpol) are now operational, and these may now become a precedent for similar identity-related crime units.

32. The protection and support of victims in general has been a focus of law reform in some Latin American States, and offices have been established to deal with victims, but there is very little expertise on the nature and needs of victims of identity-related crime *per se*. When one State did open access to services for victims of identity crime, however, the demand was substantial. There are few effective mechanisms to assist in the restoration of identity, and it is generally seen as necessary to develop expertise and services, and to raise awareness of victim-support services as they become available. There is also little law applicable to victims of identity-related crime. The *Inter American Convention on Human Rights* has good victim protection provisions, as have national laws that have implemented the Convention, but these are not specific to these particular victims.

33. On technical assistance, it was suggested that in the Latin American sub-region, this would be different in areas where technologies are highly developed and relatively less so, as the degree and nature of cybercrime and other technological involvement in various forms of identity crime are different, and the means or facilities of delivering assistance may also be different, but neither of these was seen as a serious obstacle. In general, technical assistance would have to be directed in one sense at the States *per se*, when elements such as legislative and policy development were the focus, but also on a regional basis within and among States with the regions in question being defined by the technical capacities open to exploitation by offenders and access by law enforcement. More generally, it was noted that cyber-elements of crime and crime-control are a problem everywhere, and technical assistance even in developing countries has to focus partly on the future, which entails precautions against cybercrime techniques even in places where offenders have not yet acquired the expertise or infrastructures do not permit their use. It was also noted that specialized prosecution and law enforcement units may also become a channel for the delivery and receipt of technical assistance as they are established.

34. Mr. Salt highlighted the regional need for technical assistance in several specific areas. There is a shortage of data and analysis and assistance is needed with criminological studies. Assistance is also needed with respect to the establishment and training of Computer Emergency

Response Teams (CERTS). Within the region, the reform of criminal offences is important, but reform of criminal procedure is even more so. There is also a need for assistance with respect to education and awareness-raising, as well as materials and institutions for the support and assistance of victims. One logistical advantage for the region is that all States are Spanish-speaking except for Brazil. As with the recommendations of the core group for assistance in general, the region's needs reflect a range of target audiences, which requires modular materials that are appropriate for sophisticated audiences such as legislators and prosecutors, but also more general ones. Specific target audiences mentioned included the users of social networks, groups of clients or customers of banks, credit card and similar companies, law enforcement, prosecutors and judges. This raised obvious concerns about resources and the "train the trainers" approach taken in other UNODC initiatives was proposed as a practical alternative.

35. Concerning public-private cooperation, the precedents of Europe and North America are not seen as valid for Latin America. Much more work is needed within the region to build confidence on both sides and help establish good private/public relationships. One example mentioned was the reluctance of companies responsible for maintaining websites and search engines to take an active role in identifying and suppressing the dissemination of child pornography. Legal powers for law enforcement to compel assistance and the corresponding liability of service providers to customers were also uneven across the region. Adequate legal frameworks for international cooperation exist on the basis of UNTOC and regional instruments, and any need for additional measures was seen as consistent with those for cybercrime, in view of the widespread links between the presence of technologies and transnational offences or criminal schemes. Mr. Salt suggested that good mechanisms to approach the region as a whole included *REMJA*[14] and the OAS working group on cybercrime.

IV. Agenda item 5: Specific session on the protection of victims

36. Ms. Skinnider introduced a draft outline of a manual on the "Protection of victims of identity-related crime: Guidelines for law enforcement and prosecutors", for the elaboration of which the International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR) had received funding.[15] She indicated that the target audience at this point is primarily law enforcement and prosecutors, but that it was intended also for use by policy makers. ICCLR's funding and mandate to produce the manual, and hence its focus, is Canadian, but it is hoped that it will also be useful for the core group and international users. Thus, the Canadian project will address Canadian victim perspectives, but will also benefit from expertise gathered through the core group with a view to being "internationalized" and including assessments from the U.S. and elsewhere. Given the global nature and similarities in how victims are affected a high degree of commonality seems likely. Stakeholders consulted in its development include law enforcement, prosecutors, Canada's public safety ministry, victim interest experts within and outside of governments, and relevant private sector entities. The finished version will draw in part on earlier work by Ms. Philippa Lawson on behalf of the core group,[16] as well as the results of the 2007

[14] REMJA refers to the OAS mechanism for Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (*Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas*). See http://www.oas.org/en/sla/dlc/remja/background.asp.

[15] Another document provided by ICCLR was an inventory of legal rights and remedies for identity-related crime victims in Canada. The inventory was distributed in confidence for the information of the core group and it was made clear that its contents did not necessarily represent the position of Canada, either domestically or within the core group itself.

[16] E/CN.15/2009/CRP.14.

United Nations study. It will also contain background information about the international context of crime and anti-crime activities. The draft manual consists of 7 modules. The first module serves as a basic introduction explaining what identity-related crime is, why the Manual is needed and what it can do to assist in dealing with relevant cases. It contains, *inter alia*, discussions of how to identify and locate victims, how to intervene early to minimize and prevent harm, and how to communicate effectively with victims. The second module examines the legal framework in Canada, including specific and general offences, information law, privacy and victim protection laws.

37. In discussion, Mr. Cain noted that while specific to Canada, the outline of the legal framework is also potentially useful to other countries. The rapporteur of the core group observed that an ongoing issue in identifying and dealing with victims remains the difficulty in separating the primary crimes of the abuse of identity documents or information from the secondary identity-related crimes such as fraud. From the perspective of victims reporting crime and seeking help, these cause overlapping harm and are likely to be considered as one offence. From the perspective of criminal justice statistics, law enforcement investigators and public and private sector sources of victim-assistance, on the other hand crimes such as identity theft and crimes such as fraud might trigger different responses. Mr. Rusch noted that, in identifying victims, it was important to include not only those whose identities were compromised but also victims of the secondary offences and the commercial interests against which losses were usually allocated, such as credit card companies and financial institutions. Including the latter as a class of victims helped lay the groundwork for better public-private sector cooperation in general. It was also important to look at the impact of identity crime on government agencies as victims, or at least those entities which suffer identifiable harm as a result. On the question of the discussion of definition and scope, Mr. Rusch also drew attention to recent work of the Canada – United States Cross Border Crime Forum, which produced a threat assessment this year, and to a similar recent assessment by the U.K. National Fraud Authority also did a threat assessment. He noted that a similar assessment was also being developed in Australia. Concerning the legal framework, he noted that the U.S. had previously done surveys on laws and developed samples of typically useful laws. Examination of this might be useful by comparison and assist in advising Canadian users with respect to the global nature of the problem and the specifics of what they may encounter in different countries or legal systems.

38. Ms. Skinnider then reviewed the content of module 3, which provides an assessment of typologies based on both nature of offending and by types of victim targeted. This will include corporate and other unconventional victims. Messrs. Ram and Rusch noted that it was difficult to assess what "typical" victims were, both as a result of the complexity and range of offending and the lack of statistical and qualitative data to-date in what is still an emerging crime area. It is clear there is no single high-risk group, but there could well be clusters of typical victims for specific types of identity crime. The U.S. has been collecting data from self-identified victims using reporting web-sites, but this cannot be used to identify the full range of victims or establish patterns because victim self-reporting leaves large gaps. It has now started gathering data based on surveys of general population samples, but it is too soon to identify any patterns. At this stage all that could safely be said is that some groups may be at greater risk of some types of identity crime, and that more information is needed. Some clear patterns have been noticed. For example, cases of theft and trafficking by insiders depend on the nature of information the offender has access to in the first place. Mr. Cain observed that a lot of information existed in the private sector, and much of it was available, but that it did not necessarily meet official statistical standards or reflect the same categories for collection and evaluation that governments would use. The rapporteur of the core group noted that in the context of a global research this may not be critical. Statistical information that meets the standards of the most developed Member States is

seldom available in global studies. Reported with appropriate caveats such information as is available is still a useful basis from which the core group and UNODC can develop assistance to Member States and can suggest directions for more specific research. Mr. Rusch noted that the problem was also partly a question of qualitative data. Information such as typical patterns of victimization and examples that illustrate them are needed. Individual law enforcement agencies and specialized investigative units are a good source of this data and also a good user of the advice it generates.

39. Ms. Skinnider then reviewed module 4, which examines law enforcement and investigative issues. These include various reporting scenarios setting out how crimes come to the attention of law enforcement and how victims are identified. The importance of early action, both for victim support as a crime-prevention measure to prevent ongoing/future victimization is emphasized. The means of authenticating victim claims and suggestions of how law enforcement can communicate effectively with victims are also examined. An underlying problem here is the expectation of victims and distinguishing between what can be done by law enforcement, other State entities, relevant private sector entities and by victims themselves, and Ms. Skinnider noted, in this context, that Canada was considering the establishment of a victim self-help centre. Module 4 also examines cooperation between law enforcement and private sector entities, reviewing existing arrangements and areas where cooperation is and is not possible. It will also examine best practices and will include both Canadian and other States' practices. It was noted that ICCLR was seeking input on this from experts from other countries. Mr. Cain suggested that this module could also address scenarios for data gathered from non-victims. Communications with companies and other non-victims who encounter and report crimes or who recover stolen identification is also important. He noted that it would also be very helpful to specify a basic minimum data set to include in occurrence reports and set up a reporting framework so that collected data all goes to same place. Mr. Rusch noted that while this is focused on guidance to law enforcement, it will also be very useful to victim service organizations.

40. It was further argued that the manual could also deal with some aspects of international cooperation. Mr. Rusch suggested that even for Canadian domestic use this would be helpful, and noted that it could also draw attention to the past recommendations of the intergovernmental expert group that had developed the 2007 United Nations study and the core group, both emphasizing the need for use of existing international legal instruments. In this connection, the significance of the UNTOC was highlighted, as it establishes general frameworks for mutual legal assistance and other cooperation and also encourages States parties to develop more specific and expeditious arrangements on a bilateral or regional basis, where feasible. Mr. Rusch also observed that, in view of the links between victim issues and investigation, prosecution and international cooperation, appropriate cross-references would be important, especially with the manual on international cooperation to combat identity-related crime, commissioned by UNODC in line with mandates from the core group and soon to be published. Mr. Cain emphasized the need for relatively compact and straightforward materials, particularly given that many of them would be used by victims themselves and line investigators and others who come into direct contact with victims.

41. Concerning module 5, Ms. Skinnider summarized the content, which deals with prosecution issues, including basic materials on evidence and the role and protection of victims in judicial proceedings. This module will incorporate suggestions from the core group, as well as recent and pending Canadian law amendments. Concerning prosecutors, there was discussion of various administrative models. Developed countries with relatively well-resourced prosecution services and high case-load volumes were seen as more likely to train and assign specialized prosecutors and other experts, whereas in most States, ordinary prosecutors would take on

identity crime cases in general mix of criminal offences. This meant that, to some degree, the materials needed to be directed both at specialists and generalists, especially if and when they are adapted for international use. Mr. Rusch noted that in the U.S and some other countries there were already prosecutors and law-enforcement teams specialized in related areas such as economic fraud or major economic crimes, money-laundering and organized crime who might be called upon to deal with specific cases of identity-related crime or to add expertise in dealing with such cases to their existing mandates and competences. He also suggested that, whatever the specific organizational framework, the close coordination or integration of prosecutors dealing with identity crime and identity-related crime with their counterparts dealing with general crime and other specific types of crime would be important. There was also some discussion of the complex ways in which criminal cases could arise and come to the attention of law enforcement and prosecution officials, and some of the implications of this for the collection, preservation and use of various forms of evidence. Victim-information packages could incorporate basic evidence elements, especially those intended for corporate victims, who are considered as such because they absorb losses, but who usually are in a position of becoming aware of abuses of client or customer identity and notifying both the customer and law enforcement. Awareness of such issues was seen as especially important in digital environments, where rapid preservation of evidence is essential.

42. Concerning victims, there was discussion of who should be considered as a victim, different categories of victims, and how victims could be identified in cases where identities were compromised in some way but no additional offences were committed with them or where an identity-crime scheme was interrupted by law enforcement or other disruptions before such additional offences could be completed. Mr. Rusch commented that in the U.S. the emerging practice is to treat those affected as victims and entitled to notification by prosecutors when the case reached the stage of a formal indictment. The rapporteur of the core group noted that notification requirements and practices went beyond the scope of the criminal justice system. The question of whether companies should be required to notify clients or customers that their identities had been stolen, copied or otherwise compromised is controversial in some States. Commercial interests, on one hand, tended to want to protect their reputations and not to alert or alarm customers unless absolutely necessary. Customers and victim-interest groups, on the other hand, tended to argue in favour of contractual or legislated requirements to notify on a broader basis. Mr. Rusch also commented that notification requirements could be problematic for other reasons in some cases. There have been leaks of very large numbers of personal identities in several countries. In the U.S., one case involved the identities of about 26 million veterans, rendering individual notification impracticable. It was generally agreed that any notification requirement would need to be limited to “provable” victims, and that each State would have to develop appropriate criteria to make such a standard work, especially if implemented using legislation.

43. Ms. Skinnider then reviewed the sixth module of the manual, which deals with the resources needed to support and assist victims in areas such as legal rights and recourses and practical support in self-help and dealing with commercial, law enforcement and prosecutorial institutions. She indicated that this module was directed at, and intended to be used by, victims in general, which might require refinement or supplementing with additional specialized materials as a clearer picture of victims in general and various specific sub-categories of victims emerged. There was then discussion of some of the specific actions that would be required of victims and the sorts of support and information they would need. Mr. Rusch noted that one critical need for victims in this particular area is access to legal advice. In many U.S. jurisdictions, law societies and professional bodies had established rosters of counsel willing to provide such services *pro bono*. This has proven successful, and the Federal Trade Commission had supported it by

assembling an attorney desk-book. This compiles in one easy-access package all of the relevant legislation, nature and access points to all of the various redress mechanisms, and similar information, which improves the quality of the advice, while at the same time reducing the time needed, so that *pro bono* counsel could deal with more victims. Mr. Salt raised the question of fraud-watch lists and various commercial protection schemes, which offer either proactive protection or assistance in identity-restoration for a fee, and which have become common in some Latin American States. Mr. Caine noted a similar trend in the U.S. in which customers can buy protection and monitoring over and above basic rights or customer services. Paying for protection is gradually becoming *de facto* a mandatory obligation, which has in turn become a policy issue. Mr. Rusch noted that this offered opportunities for fraud schemes, and emphasized the importance of ensuring that any government assistance is available free of charge, and that the public is made aware and constantly reminded of this fact. Ms. Skinnider observed that, apart from the risk that free services would be fraudulently "sold" to victims, it was important at a more general level to ensure that victim services were easily available and accessible to maximize utilization and reduce the risk of re-victimization or exploitation, and that this included ensuring that they were either free or offered at a reasonable cost.

44. Ms. Skinnider concluded by reviewing module 7 of the manual, which deals with policy issues. Most general policy issues were well-known to members of the core group, but policy issues specific to victims were less clear and still being defined as more is learned about identity crimes, their impact on victims and the reactions of the State, victims and private sector and other interests to them. She recalled that the 2009 paper by Ms. Lawson had highlighted a number of gaps in policy and supporting information, most of which still comes only from U.S. sources. It was noted that information was needed both to assist in identifying and clarifying victim-related policy issues and for the development of responsive policy options. This included both statistical information to identify and quantify different types of identity-related crime and of victims, and more detailed qualitative information needed to provide clear descriptions, explanations and examples of the various types of crime and victims. Mr. Rusch noted that even the U.S. does not have over-arching statistical information or the criteria on which it would be based. Most of the criteria and data used are more situation-specific. There could be various means of gauging the effectiveness of programmes, but many of the results and benefits are indirect and/or intangible. It was also noted that the data available, especially at the international level, were seldom complete and generally less than ideal, but that it was important to provide the best possible advice to Member States based on qualitative and professional assessments even if they were imprecise. Mr. Martins de Almeida also highlighted some of the problems of counting occurrences. As with other common transnational offences, there was the potential both for double counting of the same crimes in offender- and victim-jurisdictions, but also the potential to under- or over-count occurrences where identity-crime schemes also committed identity-related crime offences such as fraud. Other issues that pose challenges are related to the differences in counting offenders, offences and victims, especially in ongoing or mass-victim phishing and fraud schemes.[17] In closing on this issue, Ms. Skinnider indicated that the ICCLR hoped to complete the present project in late January of 2011, and invited members to submit any further comments electronically before then.

[17] Similar issues were considered in the course of the 2007 United Nations study. See E/CN.15/2007/8/Add.1, paragraph 18.

V. Agenda item 6: Private sector and identity security/management

45. Mr. Knopjes began the discussion with a presentation summarizing recent developments with respect to the creation and verification of identity. He described a 2008 European regulation requiring that professionals such as lawyers and notaries establish client identity, and further briefed the core group about accompanying programmes to provide training for staff on how to do this. Given the large numbers of staff to be trained, a web-based application is used, with the basic training package taking about 2 hours per trainee. A key element was the comparison of documents, and very basic *indicia* that might suggest that a document is forged, altered or, even if valid, is being used by someone other than the person to whom it was issued. Materials used include regional modules with samples of identity documents likely to be encountered in genuine or falsified forms in a particular location or profession, and updates to assess new innovations by offenders and trends that might suggest documents or contexts in which the risks of identity abuses might be elevated in the future. In essence, the objective was to sensitize staff members and enable them to make basic determinations on three key issues: "Is the document authentic?" "Is it valid?", and "Is the user the person it purports to identify?" The process also includes training and basic testing to assess qualifications and the need for further training, if any. Some of the materials and content are intended to allow front-line officials and staff members to at least tentatively identify fabricated or altered documents by visual and tactile examination (e.g. of watermarks, intaglio printing etc.), as well as the use of some of the basic devices, such as magnifiers and ultraviolet lamps, needed to view some of the more common additional security features. Some of the package is based on contextual forensic and intelligence assessment of the easiest or most common means of identity falsification in various contexts, such as the substitution of photographs and the alteration of names, dates and other basic identity information on documents, that are likely to be encountered by specific staff members or officials in specific circumstances.[18]

46. In discussion, it was noted that only a pilot project, training 15 such staff members, has been completed, but that the project had only just started operation. Aside from professional support staff, there was also the potential to expand it to other target groups of front line officials and there have been some preliminary contacts with the International Civil Aviation Organization and other interested agencies.[19] The format has also been developed so as to permit easy expansion to specialized contexts or documents in accordance with assessed needs and demand. Factors such as the gradual strengthening of international passport standards and their uptake and implementation in the various Member States can be factored in as the training progresses. In essence, there would be a standardized element on the recognition of false documents in any context and then specific materials on the misuse of particular documents in particular situations as needed.

47. The Chairman noted that in dealing with identity infrastructures and identity-management issues there was always a need to consider the relationships between public sector and private sector aspects, and that this required mutual confidence-building measures to address misunderstanding, misinterpretation and mistrust. This applied not only to the investigation and

[18] The need for such training and the engagement of forensic and criminal intelligence sources in developing and delivering it was discussed by the core group at its fourth meeting. See the report of that meeting: E/CN.15/2010/CRP.3, paragraphs 44-46, 51 and 54-55, and the report of the UNODC Laboratory and Scientific Support Section from the same meeting, E/CN.15/2010/CRP.2, paragraphs 11 and 65-70.

[19] ICAO is responsible for the development and maintenance of agreed international technical standards for machine-readable passports, and front-line airline staff is required to verify passports and other travel documents prior to allowing passengers on board international flights. See E/CN.15/2007/8, paragraph 35.

prosecution of identity offences, but also to the design and establishment of identity infrastructures and technical and situational crime prevention as well. Mr. Vancoillie noted that in Belgium, as in most European States, every resident is already registered and that these registrations have now been converted into electronic identities (eID) which are beginning to be used both for public applications such as taxation and for private commercial applications. Mr. Castellani highlighted that the same identity infrastructures could be used for public and private applications, but that this could become problematic in the context of public protections in public areas such as personal privacy and in circumstances where there are commercial abuses. Mr. Vancoillie noted that Belgium had observed a need for some degree of compartmentalization and other security precautions, including the use of eID along with other identifiers as appropriate in various circumstances. This entailed striking a balance between some reduction in overall efficiency and usefulness, and the need to protect essential interests and deter and prevent crime, but, on the whole, the State-based nature of the infrastructure made it harder for illicit interests to subvert or exploit. Mr. Cain observed that a key challenge for most private sector companies was to find ways to quickly and efficiently verify official documents and their users, and that State-operated eID systems might make this easier if this was taken into consideration in design and implementation. Another challenge in this area for both sides was to develop mechanisms that allowed private companies to verify public identification that were reliable and at the same time did not lead to over-disclosure, including disclosure of personal information and disclosure of technical security elements of documents and verification mechanisms. The same information needed to allow a private company to detect forged documents could also be used by offenders to refine their forgery techniques for example. Mr. Castellani observed that all of the work by the core group and others in this area thus far had focused on the establishment of infrastructures and documents needed to identify human beings. He foresaw that many of the same infrastructure elements and technologies being developed to identify natural persons could also be used to identify legal persons and things, such as various forms of property that warranted registration and tracing. [20] The rapporteur of the core group noted that, while domestic criminal law systems had engaged in such exercises with specific forms of property, such as requirements that firearms be marked with serial numbers and tracked in some circumstances,[21] different forms of marking and tracking would probably be needed depending on the sort of property involved and the circumstances, and that absent some compelling reason to do so, governments would not generally see this as a matter for criminal law or criminal justice systems.

48. Mr. Cain reviewed the role and recent activities of the Anti-Phishing Working Group (APWG), including providing specific information and assistance to the private sector in support of action on phishing web sites, privacy issues, user-education/prevention matters, the development and dissemination of its informational materials in languages, and the voluntary and

[20] At its first and second sessions the core group also considered questions related to the need to be able to establish the identity of legal persons as well as natural persons. This dealt with areas such as copyright and trademark infringement, which are seen as criminal law matters in some Member States and as a civil matter in others. The core group concluded that further work in this area was not a priority. See the Report of the core group at its second session, E/CN.15/2009/CRP.11, paragraph 37.

[21] See A/RES/55/255, Annex, the *Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components, supplementing the United Nations Convention against Transnational Organized Crime*. Other infrastructures for the identification of property that have engaged criminal or quasi-criminal law enforcement include schemes for the identification and tracing of nuclear materials and radiological substances and of diamonds. See A/RES/55/56 and http://www.kimberleyprocess.com/home/index_en.html (Kimberly Process for exclusion of "conflict diamonds" from markets) and the 1980 *Convention on the Protection of Nuclear Materials* http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml.

non-profit nature of the APWG. He further discussed new developments in the tactics being used against on-line phishing sites. Generally, the process consists of identifying phishing sites and taking them down as quickly as possible, but also posting anti-phishing information to be found by anyone who later visited the site, and this had led to discussions of what information could be so posted, having regard to privacy and other issues and to striking a balance between alerting potential victims while at the same time not providing information that could be useful to offenders. This has led to APWG engagement with specific agencies on how to deal with specific scams and specific counter-measures. One example provided was the use of a "rebound fax" that is sent automatically to those who fax information to a fax number that had been posing as the US Internal Revenue Service before it was taken down. A practical challenge was how to develop concise information packages which give enough information about how scams work and how not to be victimized and which do not overwhelm or overload the potential victims with information. The essence of such schemes is large volumes of vary basic information packages. Test results for the latest APWG core information package have been positive so far. Mr Caine also recounted the ongoing work of APWG in maintaining a "blacklist" of URL addresses used for spam and phishing that are updated every 5 minutes or so and used by commercial security companies to update firewall and other security applications and services sold/delivered to customers. He noted that the APWG had also tried a more interactive and intelligence-based system that would have compiled user confidence levels to generate advice to lock out doubtful or dubious sites based on the mere probability of involvement in phishing or other illicit activities. This had been tried for a few months but had proven problematic due to privacy concerns about the information it had contained.

49. More generally, Mr. Caine also reviewed some of the ongoing challenges faced by the private sector. This included the fact that there are different protection frameworks for information and different rates at which action can be taken. The private sector can usually act much more quickly, especially if more than one country was involved, but while this might disrupt or prevent crime, it generally does not meet public evidentiary or other standards needed to support prosecution. The private sector can easily identify and gather data, but for public law enforcement agencies this is a seizure, and if transnational, a matter for formal mutual legal assistance requests and responses. Often these take more time given the on-line nature of the criminal schemes involved and their ability to disappear and re-appear at will. The general pattern is that private sector information could initiate criminal investigations, but formal investigative measures have to be used after that. Even this low level of private sector involvement can be a problem, in terms of constitutional and in Europe, privacy constraints.

50. In discussion, it was noted that the APWG is not a commercial entity in the conventional sense, but a non-profit company under U.S. law. Its membership includes companies, universities, individuals, as well as some law enforcement representation in the United States and other countries. It has multiple partnerships with private constituents and various public agencies, including CERTs (Computer Emergency Response Teams). It was also noted that there is a need to commence gathering meaningful statistics, both to assess the seriousness and scope of the problem and to motivate various criminal justice and other responses to it. Qualitative information, such as sample cases and responses was also needed to assist in illustrating the problem to non-experts. In terms of cooperation in actual cases, there may be occasional circumstances in which information shared by companies would cause harm if disclosed in a prosecution, but these are fewer and less serious than the information-sharing and disclosure issues in some of the serious crime and national security cases that presently arise. More serious is the potential that private sector entities may be asked to obtain and transmit to law enforcement information that would trigger search and seizure or other procedural safeguards if done directly by law enforcement. Companies could be used to circumvent technical obstacles but not legal

constraints or safeguards. Mr. Cain indicated that law enforcement was sometimes reluctant to accept information from companies because of privacy concerns, for example when subscriber or other IP addresses are disclosed.

51. Mr. Rusch highlighted the need to identify and raise awareness of practices which are still within limits of national law, both to avoid artificially creating constraints where they are not needed, and to ensure that such constraints as exist in various circumstances are understood and applied properly. There was usually good potential for a two-way flow of information with appropriate safeguards, and also many actions short of full-blown enforcement and prosecution that could be taken by one or both sides. He noted that actions which disrupt ongoing criminal activities may still be possible even if evidentiary standards not met or available evidence is not sufficient to prosecute. There was also potential for law enforcement to alert private companies that their facilities were being compromised or misused without necessarily disclosing sources or sensitive or protected information. He noted that both the public and private sector needed to work together to solve problems, but also to identify the many existing productive partnerships which are working so they can be enhanced and replicated elsewhere. In many cases, intricate laws and expensive infrastructures are not needed to make partnerships work. One possible product for the core group could be to develop and provide a range of models or best practices at various levels of sophistication.

52. There was also discussion of the range of approaches in different legal systems to cooperation between law enforcement and the private sector. Mr. Martins de Almeida noted that there was a range of types of information and applicable requirements in different systems. Brazilian law and practice, for example, may deal differently with information that simply commences or assists investigations, information which is to be used as evidence, and information which could be considered to be criminal intelligence, in the sense that it relates more to the activities of an organised criminal group or scheme in general than as evidence of specific offences that would be prosecuted. In Brazil, there is no specific legal provision authorizing law enforcement to request information from telecommunications providers and no requirement for them to provide it. Mr. Martins de Almeida also noted that the International Standards Organization was presently developing an identity management protocol which might form the basis of links between law enforcement and service providers, or might assist States in establishing the necessary legal frameworks. Mr. Vancoillie also observed that in many systems different approaches were followed in scenarios where law enforcement asks for assistance, thereby triggering procedural and human rights safeguards, and scenarios where companies or other informants offer information on their own initiative, where the same constraints may not apply. The Chairman also noted that in many civil law States, official lists of experts authorized to assist investigating judges were established, whereas in common law States investigative measures were undertaken by law enforcement, with assistance from telecommunications providers where necessary, pursuant to court orders. Mr. Castellani observed that while the focus of the discussion was on criminal law and criminal justice mechanisms, other responses also needed to be considered. The reliability and evidentiary value of information was important for prosecutions, for example, but also for addressing claims by and against victims, establishing identity for remediation, and similar purposes. It was also noted that the nature of the communication system or expectation of privacy could make a difference in some jurisdictions. Voice communications, e-mail, SMS messages and Internet communications may be treated differently.

53. Concerning the role of UNODC and the core group itself, the Chairman commented that both the private sector and law enforcement have the capacity to cooperate but are generally uncertain as to one another's capacity and applicable constraints. One possible role for technical

assistance materials and projects could be to explain each side to the other, or at least to provide basic materials and information that could then be adjusted for each specific State or region. Mr. Cain emphasized the scope of the information and materials that would be needed, including everything from sophisticated technical training to very basic education of judges about how computer systems work. Mr. Rusch noted that many measures directed at the law enforcement investigative process would not need to be developed, as there are already systems in place for this. Instead, the challenge is more about general reciprocal sharing of the sorts of information needed to enhance security and take other measures to prevent, disrupt, and generally combat and suppress this sort of crime. The main issue, in this regard, is not to facilitate the sharing of investigative information at the operational level, but to help those who do perform this function to identify information, factual scenarios and other circumstances which either require that formal safeguards be applied, or which permit more expedited and informal cooperation when safeguards are not required. The rapporteur of the core group noted that, in developing global information and materials a range of other fundamental issues would also need to be addressed. Different States have different concepts of the private sector and of where the demarcation between public and private activities should be located. Telecommunications services may be seen as a matter for private companies in some States and as public infrastructure in others, for example. There is also a wide range of specific commercial activities, carried on by companies of a small local nature or by large multinational corporations, which raise differences in capacity to cooperate and in applicable legal safeguards or other constraints in the various jurisdictions in which a company operates. Mr. Murungi noted that the basic structure of the private sector varied widely. In developing countries, both companies and technologies are smaller and less elaborate and the ability to cooperate can be more limited. Non-profit and umbrella companies or organizations such as the APWG are not typical in such regions. Small private companies are not actively engaged in anti-crime activities and would probably require both encouragement to play such a role and assistance to help them to develop the capacity to do so.

54. It was noted that one key objective was to provide reassurance and build confidence. Companies share the objective of preventing and combating crime and are often willing to cooperate, but they require some legal reassurance. In the U.S., for example, companies want subpoenas to cover them from claims, and these often cannot be obtained in the early stages of an investigation because sufficient evidence has not yet been collected. If the companies had more reassurance they might be able to volunteer the information at an earlier stage. Mr. Vancoillie noted that those who witness isolated crimes and report them to law enforcement did note raise concerns, but legal issues were more likely to arise if there were an established relationship, as was often the case with companies, even if it is the company that volunteers the information. Mr. Rusch also offered an example to illustrate the differences between specific and general information. In the U.S., law enforcement investigating a group of offenders moving from city to city and committing identity and credit card frauds noted a pattern in their use of rental cars. They were able to persuade a car rental company to watch for the same pattern and alert authorities when it was detected in another city without disclosing any sensitive information or requirements for judicial oversight.[22] This sort of information is often not about "who", but about "how". It can usually be freely shared and it can be extremely useful in putting law enforcement into situations where they can start investigations on their own at an early stage.

[22] The potential for using the analysis of suspicious patterns of activity to identify possible targets for criminal investigations without triggering human rights or procedural requirements was considered by the intergovernmental expert group as a means of identifying possible mass fraud schemes. See E/CN.15/2007/8/Add.2, paragraph 30. The core group also considered the value of forensic assessment as an element of pattern analysis to support criminal intelligence and direct investigative focus and resources in identity-related crime cases at its fourth session. See E/CN.15/2010/CRP.3, paragraph 51.

55. In conclusion, several additional issues were raised. The continuing challenge of both persuading the private sector to provide data about both technological and crime trends and of evaluating and reporting such data was raised. Generally, the core group saw this as a critical issue for the forthcoming cybercrime study process and noted that while some progress has been made, much more was needed. Mr. Ram noted that the core group could serve as a precedent and an example of a mechanism that works, to demonstrate that effective cooperation is not only necessary, but also possible. While it contains mostly information shared between law enforcement agencies, Messrs. Cain and Knopjes both drew attention to the Interpol database of stolen travel and identity documents as an example of effective information-sharing. Established in 2002, Interpol now indicates that it compiles over 20 million stolen documents, against which suspect documents can be checked in real time.[23]

VI. Agenda item 7: Technical assistance - International cooperation

56. In opening discussion on this issue, the Chairman highlighted the need to provide for the possibility of incorporating private sector information and resources into the development of materials (as the core group is presently doing) and also in the delivery of technical assistance projects. There was also discussion of the ethical and practical implications of drawing on private sector expertise and resources. While these were seen as useful in enhancing quality and essential to ensuring that technical assistance covered private sector aspects of crime-prevention, investigative cooperation and other matters, it would also be essential to ensure that the credibility and independence of the United Nations were not compromised and that supporting commercial entities did not gain competitive or other advantages as a result of their participation. It would be important to ensure that the motive to support and collaborate in the work was to prevent and suppress crime and not to advance commercial interests globally or in any specific Member State. The United Nations banner would impose some constraints on how resources were collected and used, but at the same time it provided credibility and a delivery framework that were seen as essential to the effort.

57. Mr. Rusch noted the need for a clear over-arching strategy that was acceptable to Member States, and various means of informing and reassuring them that what was actually done fitted within that strategy. He also stressed that, from a governmental standpoint, it would be important to clarify in advance the extent to which Member States themselves would contribute experts and support the work. It was also noted that, on one hand this needed a fixed package of materials and fairly standard projects, but on the other, some capacity to be flexible in targeting different States and audiences was needed to respond fairly quickly to specific requests for assistance. It was underscored that elements dealing with either economic fraud, identity-related crime or both could be the focus of technical assistance projects or could be incidental elements of projects directed at other problems such as organized crime or money-laundering. Projects could be convened and run by UNODC, or UNODC could provide support for projects initiated by Member States or regional or sub-regional organizations. Attention was drawn to paragraph 41 of the Salvador Declaration, which calls on UNODC to engage in capacity-building in the area of cybercrime.

58. Discussing the means of delivering technical assistance, Mr. Cain reviewed problems and successes of the APWG. He noted that developing an overall structure and then tailoring specific modules to specific issues and audiences, while at the same time keeping the materials simple and easy to access was a challenge. The Internet and web-based delivery offered enormous economies

[23] See Interpol, http://www.interpol.int/Public/ICPO/FactSheets/GI04.pdf.

and left recipients with extensive resource materials, but the lack of interactive discussions and human contact reduced effectiveness. The Chairman noted that UNODC's experience with technical assistance projects had been exclusively directed at governments thus far, but that assistance with respect to identity-related crime might also have to be developed for and directed at some private sector entities. The rapporteur of the core group observed that the traditional role of UNODC had been more to broker technical assistance, in the sense of organizing projects and meetings to bring together experts from States which had the necessary knowledge with those in States that had requested the assistance and needed access to the expertise. There was no reason this same process could not include private sector experts. It would require both human and financial resources and these could also be mobilized in both the public and private sectors. The core group itself already possesses some of the necessary expertise: Mr. Knopjes noted that he presently provides such assistance to ICAO, and Mr. Cain plays a similar role in assisting with the training of computer incident response teams.

VII. Agenda items 8-9: Mapping out a course of future action for the core group – Conclusions/recommendations

59. Regarding the future work of the core group, the Chairman noted the forthcoming first session of the open-ended intergovernmental expert group to prepare a study on cybercrime, in January 2011, the UNCITRAL Colloquium including identity management in February 2011, and the 20th session of the Commission on Crime Prevention and Criminal Justice, in April 2011. He suggested that a brief text be prepared on behalf of the core group and submitted to the cybercrime group for is information. Furthermore, it was stressed that the present report would be submitted to the Commission on Crime Prevention and Criminal Justice at its twentieth session in April 2011 as a Conference Room Paper (CRP). Moreover, pursuant to ECOSOC resolution 2009/22, the secretariat was also mandated to submit a progress report on the work of the secretariat on economic fraud and identity-related crime which would include a review of the work and outputs of the core group.

60. In discussion, Mr. Rusch suggested that an outline summarizing elements of a national strategy on identity-related crime be prepared, if possible for the cybercrime process or for the information of the Commission on Crime Prevention and Criminal Justice. He also noted that such strategies were called for by ECOSOC resolution 2009/22, subparagraph 6(f), and that several Member States had developed or were in the process of developing them. A short paper summarizing possible elements and reasons why States could consider the development of strategies and the inclusion of various elements would not be prescriptive in nature, but could be very useful to Member States and at the same time provide a convenient summary of the scope of the work of the core group and Member States in the area of economic fraud and identity-related crime. Apart from its intrinsic value, this might also assist in informing the forthcoming cybercrime process of what has been done and the state of progress with a view to avoiding any unnecessary duplication of work.

61. With respect to the UNCITRAL Colloquium, Mr. Castellani noted the informal nature and broad scope of the Colloquium, which will not deal with identity crime *per se* and will address identity- management schemes only in the context of their role in electronic commerce. Several members of the core group expressed the view that identity-related crime was an issue related to identity-management and/or e-commerce, and that the Colloquium should probably be reminded of this, even if crime is not seen as a major issue. Mr. Knopjes noted that work is presently underway in several *fora* on identity-management issues, and there was a need for greater

coordination, to avoid duplication and to help ensure important elements such as crime prevention, were not left out.

62. Several members of the core group raised the need for future coordination of the core group's meetings with those of the expert group on cybercrime. They recommended that, as long as the work of the cybercrime expert group continues and holds annual sessions, the core group meetings should be held in adjacent time periods if possible, so as to minimize travel time and costs and better use available resources. It was agreed that, if there is a meeting of the cybercrime expert group in late 2011 or early 2012, and if feasible, the sixth meeting of the core group would be held in conjunction with that meeting.

63. A series of the other documents produced or updated by core group members were included in a publication entitled "Handbook on identity-related crime", which will be released in time for the twentieth session of the Commission on Crime Prevention and Criminal Justice in April 2011.

64. It was proposed that the focus of the sixth meeting of the core group would be on technical assistance issues, and in particular the various issues raised by engaging the resources and expertise of the private sector in the development and delivery of technical assistance. Apart from the questions raised by commercial entities, Mr. Murungi noted that the scope of "private sector" and the extent to which it included non-commercial elements of civil society would be a factor for consideration. The rapporteur of the core group drew attention to earlier decisions to the effect that technical assistance materials should be modular, in part to facilitate such integration and in part to enable use to target different audiences in different Member States or regions.