Economic and Social Council

Distr.: General
19 February 2013

Original: English

Commission on Crime Prevention and Criminal Justice
Twenty-second session
Vienna, 22-26 April 2013
Item 7 of the provisional agenda[*]
World crime trends and emerging issues and responses in the field of crime prevention and criminal justice

Note verbale dated 19 February 2013 from the Permanent Mission of the Argentine Republic to the United Nations (Vienna) addressed to the United Nations Office on Drugs and Crime

The Permanent Mission of the Argentine Republic to the United Nations (Vienna) presents its compliments to the United Nations Office on Drugs and Crime and has the honour to forward, pursuant to Economic and Social Council resolution 2011/35 of 28 July 2011, the report of the sixth meeting of the core group of experts on identity-related crime, which was held in Vienna from 16 to 18 January 2013, with the request that it be made available as an official document of the twenty-second session of the Commission on Crime Prevention and Criminal Justice, to be held in Vienna from 22 to 26 April 2013.

The Permanent Mission of the Argentine Republic to the United Nations (Vienna) avails itself of this opportunity to renew to the United Nations Office on Drugs and Crime the assurances of its highest consideration.

[*] E/CN.15/2013/1.

Annex to the note verbale dated 19 February 2013 from the Permanent Mission of the Argentine Republic to the United Nations (Vienna) addressed to the United Nations Office on Drugs and Crime

Report of the sixth meeting of the core group of experts on identity-related crime

Vienna, 16-18 January 2013*

I. Introduction

1. Following the release in 2007 of the United Nations study on "fraud and the criminal misuse and falsification of identity", commissioned by UNODC and submitted to the Commission on Crime Prevention and Criminal Justice at its sixteenth session,[1] and on the basis of its mandates arising from ECOSOC resolutions 2004/26 and 2007/20, UNODC has launched a consultative platform on identity-related crime. The aim of this platform was to bring together governmental experts, representatives from the private sector, as well as academic experts and representatives from international and intergovernmental organizations, to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime. The platform has become operative through the proceedings of a core group of experts, which was established in 2007.

2. At is previous five meetings, the core group had provided a series of guidelines and directions for future activities which include, among others, the undertaking of further research; more enhanced consultations with the private sector; the elaboration of research papers; the compilation of examples of relevant legislation; the development of materials on best ways and means to promote international cooperation to combat identity-related crime; and the compilation of best practices for the protection of victims. Moreover, the work of the core group resulted in the release of a *Handbook on Identity-related Crime* (2011), also containing a practical guide to international cooperation to combat identity-related crime, which is intended to be used as resource material in technical assistance programmes and capacity-building activities with a view to increasing expert knowledge to address legal, institutional and operational issues pertaining to identity-related crime.[2]

3. In its resolution 2011/35 of 28 July 2011, the Economic and Social Council acknowledged the efforts of the United Nations Office on Drugs and Crime to facilitate the work of the core group of experts on identity-related crime.

4. In the same resolution, the Council further requested the United Nations Office on Drugs and Crime to continue its efforts, in consultation with the United Nations Commission on International Trade Law, to promote mutual understanding and the

* The present report has not been formally edited.

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

[2] More information on the work of the core group at its previous meetings is available at www.unodc.org/unodc/en/organized-crime/emerging-crimes.html#Identity_related_crime.

exchange of views between public and private sector entities on issues related to economic fraud and identity-related crime and, in particular, to focus the future work of the core group of experts on identity-related crime on, among other things, the various issues raised by engaging the resources and expertise of the private sector in the development and delivery of technical assistance in this field.

5. In resolution 2011/35, the Council also requested the United Nations Office on Drugs and Crime to continue its efforts, through the core group of experts on identity-related crime, to collect information and data on the challenges posed by economic fraud and identity-related crime in different geographical regions.

6. The sixth meeting of the core group was convened from 16 to 18 January 2013 in Vienna, in line with the mandates contained in ECOSOC resolution 2011/35.

II. Organization of the meeting

A. Opening of the meeting

7. The meeting was opened on 16 January 2013 by the Director of the Division for Treaty Affairs of the United Nations Office on Drugs and Crime, who thanked the participants for their attendance and referred to the background work of the core group. He emphasized that the composition of the core group was based on a multi-stakeholder approach to facilitate the exchange of views, information and expertise among different stakeholders, as well as promote their mutual understanding and cooperation in the fight against identity-related crime. He further highlighted the success of the core group in bringing the issue of challenges posed by identity-related crime as a distinct "new and emerging" form of crime at a prominent place in the agenda of various international fora in the field of crime prevention and criminal justice (Commission on Crime Prevention and Criminal Justice, United Nations Congress on Crime Prevention and Criminal Justice, Conference of the Parties to the United Nations Convention against Transnational Organized Crime and Conference of the States Parties to the United Nations Convention against Corruption).

8. In his opening remarks, the Chairman of the core group, Ambassador Eugenio Curia, representative of the Government of Argentina in Vienna, recalled the legal mandate for the organization of the meeting and made a brief introduction to each of the topics of its agenda.

B. Attendance

9. The meeting was attended by the following experts:

(a) Public sector

Eugenio Curia, Ambassador, Permanent Representative of Argentina to the United Nations (Vienna), Argentina (Chairman of the core group); *John Unsworth*, Deputy Director — Head of Intelligence and Interventions National Fraud Intelligence Bureau (NFIB), City of London Police, United Kingdom; *Jonathan Rusch*, Deputy

Chief for Strategy and Policy, Fraud Section, Criminal Division, Department of Justice, United States of America;

(b) Private sector

Anko Blokzijl, Chairman, Safran Morpho, Netherlands; *Fons Knopjes*, ID Management Centre, Netherlands; *Pat Cain*, Resident Research Fellow, Anti-Phishing Working Group (APWG), United States of America*; Ferdinand Piatti*, Price Waterhouse Coopers, Austria; *Sébastien Saillard*, International Project Manager, RESOCOM (France); *Matthew Allen*, Director-Financial Crime, British Bankers Association (BBA), United Kingdom; *Andrew Webster*, Senior Global Financial Crimes Compliance Manager (EMEA), British Bankers Association (BBA), United Kingdom; *Jonathan Shatford*, Head of Investigations (EMEA), British Bankers Association (BBA), United Kingdom;

(c) International and intergovernmental organizations

Jae Sung Lee, Secretary of Working Group IV — E-commerce, United Nations Commission on International Trade Law (UNCITRAL); *Kate Lannan*, Legal Officer International Trade Law Division Office of Legal Affairs, United Nations Commission on International Trade Law (UNCITRAL); *Christopher Hornek*, Travel Document Security Programme Manager, Action against Terrorism Unit (ATU), Transnational Threats Department (TNTD), Organization for Security and Cooperation in Europe (OSCE); *Paul Picard*, Counter-Terrorism Officer, Organization for Security and Cooperation in Europe (OSCE);

(d) Academia/individual experts

Gilberto Martins de Almeida, Martins de Almeida Advogados, Brazil; *Marco Gercke*, Professor of Criminal Law, University of Cologne, Germany; *Nikos Passas*, Northeastern University, School of Criminology and Criminal Justice, Boston, United States of America;

(e) Secretariat

Dimosthenis Chrysikos, Crime Prevention and Criminal Justice Officer, UNODC/DTA/CEB/CSS; *Armaud Chaltin*, Associate Crime Prevention and Criminal Justice Officer, UNODC/DTA/CEB/CSS; *Steven Malby*, Drug Control and Crime Prevention Officer, UNODC/DTA/OCB/CSS.

C. Adoption of the agenda

10. The meeting adopted the following agenda:

 1. Opening of the meeting
 2. Adoption of the agenda and organization of work
 3. Identity-related crime and cybercrime
 4. Comparative approaches: Challenges posed by identity-related crime in different geographical regions

5. Basic elements of a national identity-related crime strategy: Indicative examples

6. The work of other international and intergovernmental organizations

7. Technical assistance

    (a) Areas for intervention: legislative responses, identity management and prevention of identity-related crime

    (b) The engagement of the private sector in the development and delivery of technical assistance: public-private partnerships

8. Presentation of indicative examples of academic projects involving aspects of prevention and detection of identity-related crime

9. Other matters

10. Conclusions — recommendations for future action

III. Deliberations

A. Identity-related crime and cybercrime

11. The Secretariat briefed the participants about the progress made in relation to the work of the intergovernmental expert group on cybercrime.[3] It was recalled, in this connection, that in its resolution 65/230 of 21 December 2010, the General Assembly endorsed the Salvador Declaration on "Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World", as adopted by the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. In that resolution, the Assembly requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration, an open-ended intergovernmental expert group, to conduct 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.

12. The first meeting of the intergovernmental expert group on cybercrime was held in Vienna from 17 to 21 January 2011. At that meeting, the expert group reviewed and adopted a collection of topics and a methodology for the study. The methodology for the study provided for the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and academic institutions. Replies to the questionnaire were received from 69 Member States from different regional groups. In addition, 50 companies also provided feedback. Information gathering was conducted by the Secretariat in accordance with the methodology from February 2012 to July 2012. The Secretariat further drafted an Executive Summary of the draft study, based on information gathered, for consideration by the second meeting of the intergovernmental expert

[3] See also E/CN.15/2013/24.

group on cybercrime, to be held from 25 to 28 February 2013 in Vienna.[4] The status of the study will be decided by the intergovernmental expert group.

13. Information on cybercrime criminal laws was gathered through the study questionnaire, as well as by primary source analysis of legislation from more than 100 countries. The study questionnaire referred to 14 acts commonly included in notions of cybercrime. Countries described widespread criminalization of these 14 acts, with the primary exception of spam offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia, and online solicitation or 'grooming' of children.[5] For these 14 acts, countries reported the use of cyber-specific offences for core cybercrime acts against the confidentiality, integrity and accessibility of computer systems. For other forms of cybercrime, general (non-cyber-specific) offences were more often used. Both approaches were reported, however, for computer-related acts involving identity offences. Focusing on the latter offences, the target of reported crimes varied and included personal data and identification information.

14. It was noted that law enforcement globally perceived increasing levels of cybercrime, as both individuals and organized criminal groups exploit new criminal opportunities, driven by profit and personal gain. Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and "cashing out" of financial information.

15. The study also showed that individual cybercrime victimization is significantly higher than for "conventional" crime forms. Victimization rates for online credit card fraud, identity-related crime, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17 per cent of the online population for 21 countries across the world — compared with typical burglary, robbery and car theft rates of under 5 per cent for these same countries. Cybercrime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries.

16. The core group stressed the need for addressing effectively the use of sophisticated schemes to commit cybercrime offences involving the criminal misuse and falsification of identity. One participant referred to the significance of victims protection and awareness-raising programmes in view of the increasing number of cases where citizens do not take precautions to protect themselves adequately. Some participants highlighted the necessity of capacity building to enhance national capabilities to deal with such offences particularly in developing countries.

[4] See UNODC/CCPCJ/EG.4/2013/2.

[5] Illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal data interference or system interference; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright and trademark offences; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution or possession of child pornography; computer-related solicitation or 'grooming' of children; and computer-related acts in support of terrorism offences.

B. Comparative approaches: challenges posed by identity-related crime in different geographical regions

17. In line with practice established at its previous meetings, the core group was used as a platform for a comparative presentation of issues pertaining to identity-related crime in different geographical regions. In this framework, two speakers were introduced: Prof. Marco Gercke presented the developments on identity-related crime in the European Union, the Caribbean region and the Asia and Pacific region. Mr. Gilberto Martins de Almeida presented the new legal framework on cybercrime and identity-related crime of in Brazil.

18. Prof. Gercke first highlighted that, although within the European Union criminal law remains for its main part a state-driven process, the Lisbon Reform Treaty for the first time provided the EU bodies with a strong mandate outside mere intergovernmental cooperation in the area of criminal law, including cybercrime. Work is currently underway on a draft directive against child pornography and a draft directive against attacks against information systems. Similarly, article 77 of the same Treaty provides for a mandate on "Policies on Border Checks, Asylum and Immigration", which also involves issues pertaining to safeguarding the integrity and security of identity-related documents.

19. The 2010-2014 Action Plan adopted by the European Union to implement the Stockholm Programme on an "Open and Secure Europe Serving and Protecting Citizens"[6] gives the mandate to consider submitting new legislative proposals, including on cybercrime and network information security. On this basis, a "Study for an Impact Assessment on a proposal for a new legal framework on Identity Theft" was launched in 2012. The draft study was recently submitted to the European Commission. Its content took into account the work of the core group, as UNODC was asked to provide feedback in the preparatory stage of compilation of information. Prof. Gercke was of the opinion that identity-related abuses could not be effectively criminalized per se without a unified identity management scheme and that the member states of the European Union would not be ready as yet to take such a step.

20. Prof. Gercke also presented three joint projects of the European Union and the International Telecommunication Union (ITU) aiming at the harmonization of legislation on cybercrime in the Caribbean region, the Pacific Island countries and the Sub-Sahara African region, through the elaboration of model laws and technical assistance for their implementation in each country. The first project in the Caribbean region, which is now close to completion, started with a complete review of the legislation of the selected 15 countries, as well as a regional comparative study, and involved national experts throughout the process. A strategy for the implementation of the new legislation in each country was also elaborated. The Caribbean project has been focusing on enhancing competitiveness through the harmonization of ICT policies, legislation and regulatory procedures. A constructive approach led the targeted countries to the adoption of standards on cybercrime going beyond those of most European countries. The sustainability of the project was ensured by involving from the early stages national experts throughout the process, and providing them with specific training. The role of country offices to identify the

[6] See Official Journal of the European Union, C 115/1, 4 May 2010.

relevant actors was stressed as a key factor for success. The lessons learned from this processes are available on the ITU website.

21. The same approach is also followed in the second and the third project presented by Prof. Gercke. The second project was launched in 2011 upon request of the Pacific Island countries for the provision of capacity building and training in the field of ICT policies and regulations. The third project in Sub-Sahara Africa aims at the harmonization of ICT policies in the region and was launched early 2012.

22. In follow-up discussions, the participants stressed the importance of developing such standards, and in particular model laws, and stressed the role that the United Nations could have in this regard. It was also underlined, however, that the countries that already have legislation would also need awareness-raising processes and trainings on the implementation of these standards.

23. Mr. Gilberto Martins de Almeida presented the evolution of the "legislative landscape" in Brazil with regard to cybercrime. After a brief historical overview, he focused on the recent "wave" of normative action through an integrated approach. Challenges posed by identity-related crime necessitated this development given that, as it was reported, every 15 seconds a consumer in Brazil becomes a victim of identity-related crime. The most common forms of identity-related crime encountered include identity theft through targeting credit cards; the purchase of electronic goods and of mobile phones; and the opening of bank accounts based on false or misused identification information. It was stressed that identity-related crime shifted from the use of viruses to scanning, that is the use of a robot searching vulnerabilities. It was also highlighted that the origin of the attacks was mainly national.

24. The Brazilian legislative initiative is composed of a package of 11 Bills, some of which were already approved (on cybercrime and civil liberties). For the rest of the legislation, including the freedom of information act, cybercrime laws, personal data protection act, electronic transactions act, e-commerce (consumer code), m-payment act, mew IP laws, procedural (and technical) standards and regulatory rules (Security, SEC), consultations for finalization and approval are at an advanced level.

25. The two approved Bills were adopted the same day in December 2012. They complement each other, as the first one addresses more substantive issues, while the other deals with matters of procedural nature. The complementarity of the two pieces of legislation is meant to pursue a coherent approach. This is further demonstrated by the same terminology used in each of these laws, the fact that they were drafted taking into account the same international standards (such as the ISO standards), as well as the common objective of providing for both preventive and repressive measures.

26. Mr. Martins de Almeida reported that the definition used in the approved Bills covered both invasion and installing vulnerabilities in order to obtain an illicit advantage. Aggravating circumstances are foreseen for those who produce, offer, distribute, sell or spread a device or computer programme to obtain such an illicit advantage, if the content from private e-communications, trade secrets or confidential information is obtained, or unauthorized remote control of the device is achieved, or, in case of disclosure, the content of the obtained information is commercialized or transferred to third parties as commodity. A single platform to

establish and monitor standards was established for the different national institutions.

C. Basic elements of a national identity-related crime strategy: Indicative examples

27. Under this agenda item, presentations and discussions revolved around the development of a framework on the basic components of a national strategy on the prevention, investigation, prosecution and punishment of identity-related crime. In this connection, the Secretariat stated that the issue of the development of a national strategy on identity-related crime was first raised by the Economic and Social Council in its resolution 2009/22 (para. 6(f)). The Secretariat further presented a paper which had been prepared by the Rapporteur of the core group, who was not present at the meeting.[7] The paper provided an overview of the possible stakeholders or participants in a national strategy, from both the public and the private sector. It also delineated the process that needs to be followed in developing, implementing and maintaining a national strategy. Moreover, the paper highlighted the substantive components of a national strategy, focusing particularly on the initial phase of a threat assessment and compilation and analysis of pertinent information; the priority setting and coordination; the legislative elements; the investigative and law enforcement component; the prevention pillar; capacity-building; resource-related issues; and mechanisms to enhance the cooperation between the public and the private sector.

28. The national strategy adopted by the United States of America to address the challenges posed by identity-related crime was presented by Mr. Jonathan Rusch. The United States enacted in 1998 the Identity Theft and Assumption Deterrence Act, which established, for the first time, identity theft as a specific criminal offence. The following year, an Identity Theft Subcommittee of the Attorney General's White Collar Crime Committee was created. In 2006, a Presidential Identity Theft Task Force was established under the chair of the Attorney-General. The Task Force adopted a strategic plan in 2007.

29. The strategy focuses on the three phases of the "life cycle" of identity theft (attempt to acquire the victim's personal information; misuse of the information acquired; and enjoyment of the benefits of the crime while the victim realizes the harm). The strategy itself develops key areas for improvement, including the following: prevention (protecting sensitive data and making it more difficult for offenders to use the data stolen); victim recovery (assisting the victim in recovering from the crime); deterrence through more aggressive prosecution and punishment.

30. With regard to prevention solutions in the public sector, Mr. Rusch referred to practices aiming at decreasing the unnecessary use of social security numbers, as well as to educational programmes for federal agents on data protection and on ensuring an effective response to abuse of data. Similarly, solutions were identified for the private sector, such as the establishment of standards for data protection and breach notice requirements, the development of comprehensive records of social security numbers used in the private sector, better education on data protection,

[7] See E/CN.15/2013/CRP.2.

investigations on data security violation and awareness-raising campaigns. As far as victim recovery is concerned, the strategy focuses on the following priorities: training of officers offering direct assistance to victims; individualized assistance to victims; amending the criminal restitution statutes to ensure that victims recover the value of time spent in trying to remediate harm suffered; and assessing the efficiency of tools available for victims. In the area of law enforcement, the strategy focuses mainly on coordination and information-sharing, including through creating a national centre, using the same report form and enhancing exchange of data and information (currently about 40 States have their own standards for reporting identity theft). Other priority activities in the field of law enforcement include the increased prosecution of identity-related crime, as well as the coordination with foreign law enforcement counterparts, together with trainings and follow-up action to measure the success of law enforcement.

31. Mr. Rusch further reported that the increased involvement of organized criminal groups in identity-related crime cases is also a concern which is taken into account in the strategy. One of the difficulties encountered, in this connection, is the use of documents for identification purposes beyond their original purpose. It is therefore important to understand how organized criminal groups are operating in order to ensure more adequate responses. It is also important to reach out to the private sector to establish a practical set of joint responses.

32. To follow-up on the U.S. strategy, an Identity Theft Enforcement Inter-agency Working Group was established in 2008 holding meetings on a monthly basis as well as briefings by private sector researchers. An International Identity Crime Working Group was also set up with the participation of Canada, United Kingdom and United States of America. Some of the recommendations made by the core group were also taken into account. Altogether, the speaker’s assessment was that the current situation in the fight against identity-related crime is better since the adoption of the aforementioned policy measures, yet not entirely satisfactory. Therefore a regular assessment of the work done is fundamental.

33. Mr. John Unsworth presented the work of the U.K. Home Office with regards to identity-related crime. The National Fraud Intelligence Bureau was entrusted to update the assessment already made in 2010 in the field of identity-related crime. The work was conducted in partnership with all national enforcement forces, private sector partners and Home Office departments. Gathering complete information on pertinent issues remains a challenge and therefore the relationship with other sectors is pivotal. Although the public increasingly recognizes the threat, a lot remains to be done with regards to protection. Identity-related crime is also linked to other crimes, including organized crime. Mr. Unsworth reported that, according to the assessment, approximately 1.8 million people become victims of identity theft each year (one every 20 seconds). Yet, a large portion of these crimes are probably not reported. Another consequence is that around £2.5 billion are overpaid in tax credits due to fraudulent practices.

34. Mr. Unsworth stressed that law enforcement authorities often focus on the end crime and might miss opportunity to target directly identity-related crime which has occurred at prior stages of the criminal activity. The Home Office recognizes the need for a cross sector approach and for more streamlined action to fully address the threats posed by this form of crime. In this context, a cross sector strategy was developed by the Identity Crime Strategic Implementation Board (SIB), pursuing

objectives at different levels such as: securing the integrity of documents (strengthening business and public sector capability to verify and authenticate identification information, whether online or in person); enhancing enforcement measures (effective targeting of resources to disrupt the criminal activities engaged in the creation, theft and distribution of false or assumed identities); fostering prevention (sharing recovered false identity data with the public and private sectors to prevent crime); and promoting educational programmes (awareness-raising to enable and empower individuals and businesses to protect themselves). There is regular follow-up on this strategy to ensure its implementation.

35. Following the presentations, the participants agreed that the existence and implementation of national strategies to prevent and combat identity-related crime could play a valuable role in directing attention and resources and ensuring that they are used in ways which are efficiently coordinated with efforts against crime in general, with other public interest objectives and with the activities and interests of the private sector. Such national strategies can also play a significant role at the international level, clarifying the policies, laws and strategies of each country and forming the basis of discussions or negotiations on coordination and cooperation among Member States. This is particularly important with regard to identity-related crime because of the wide range of security, economic and personal functions and interests it affects and the fact that most of the problem now occurs on-line and in digital systems. The participants further agreed that the details of such strategies would vary from one Member State to another, but, at a minimum, a core list of strategic elements could form the basis that each State may wish to consider in developing such a strategy.

36. In this regard, the participants discussed the content of a short draft outline of elements for inclusion in national strategies for the prevention, investigation, prosecution and punishment of identity-related crime. This outline was prepared by the Secretariat on the basis of the Rapporteur’s paper (see para. 27 above) and the discussions on the examples of national practices referred to under this agenda item. The core group made certain proposals regarding the structure and content of the draft outline, which, as finally agreed upon, is attached to the present report (see appendix II). The core group also decided that the paper prepared by the Rapporteur be further refined and updated and submitted to the Commission at its twenty-second session as Conference Room Paper. The Commission may wish to consider both the outline and the Conference Room Paper as guidance tools and further invite Member States to provide the Secretariat with feedback reflecting their own perspective on the issue of a national strategy against identity-related crime.

D. The work of other international and intergovernmental organizations

37. Mr. Christopher Hornek and Mr. Paul Picard presented the OSCE activities in the area of identity management. Various departments of the OSCE address the problem from different perspectives such as the ODIHR with regards to migration (civil registration and population registration) or elections (voters databases), or the Economic and Environmental Division with regards to good governance and migration management. However, the sector mainly involved is the Transnational Threats Department, and in particular the anti-terrorism Unit. The OSCE work

focuses on practical aspects pertaining to the issuance of the document, its handling, the strengthening of identity management, the promotion of the upgrades of documents, including the promotion of ICAO standards, and the detection of false documents in border controls.

38. The OSCE also participates in various working groups on the topic and has completed over 55 projects since 2003, in cooperation for some of them with ICAO, Interpol, IOM, EU and ISO. The OSCE has been implementing long term projects in Moldova, Tajikistan, Uzbekistan and Kyrgyzstan. In addition, the ICAO Public Key Directory was briefly presented. It is available for free on the internet, yet uploading documents has a cost. In conclusion, it was stressed that challenges were still existing and needed to be addressed with a view to improving identity management and bringing border control up to speed.

39. Mr. Jae Sung Lee presented the work of the United Nations Commission on International Trade Law (UNCITRAL) on identity management. UNCITRAL has been a pioneer in developing international standards on e-commerce which influenced national legislations. In this regard, indicators were adopted in 2008 on commercial fraud. With the increased use of e-communications in international trade, almost all the UNCITRAL working groups are considering related issues when deliberating their respective topics. They do focus on the trade facilitation aspect of identity management, but have not adopted specific text on this issue. The IV working group on e-commerce has addressed during its October 2012 meeting issues of identity management. The group has developed a model law on e-commerce, which contains a general outline of identity management, as well as model legislation on e-signature. The group further addressed the notion of identity management system, its business model, processes and main actors as well as potential benefits. Such identity management systems are designed to identify and authenticate the users seeking access to services, as a tool to improve trust in e-commerce. A colloquium was held in 2011 that resulted in a wide consensus on the relevance of identity management to facilitate cross-border electronic transactions. It was suggested then that UNCITRAL could be in an ideal position to work on transnational legal aspects of identity management. Such work would also clarify the scope of provisions on legal signatures contained in existing UNCITRAL texts, and would facilitate the treatment of identity management in the context of other topics potentially of interest for UNCITRAL. The IV working group was therefore mandated to work on identity management in the field of electronic transferable records. It is noteworthy that the Identity Management Legal Task Force of the American Bar Association submitted a paper for possible discussion at the working group providing a general overview of identity management, its role in electronic commerce and relevant legal issues, as well as barriers.

40. UNCITRAL currently focuses on monitoring the various initiatives with regards to identity management, in order to better define the terms of a possible future mandate for the working group. UNCITRAL further collaborates with the European Union on a proposal for “Regulation on electronic identification and trust services for electronic transactions in the internal market”. Other activities include the creation of a European e-identity interoperability platform (Secure Identity Across Borders Linked); cooperation with the IOM on border management issues; cooperation with the Organization for the Advancement of Structured Information

Standards on identity commerce; and the creation of a Pan-European Public Procurement online programme.

E. Technical assistance — areas for intervention: legislative responses, identity management and prevention of identity-related crime

41. The core group recalled previous mandates calling for technical assistance in the field of identity-related crime (see paras. 7-8 of ECOSOC resolution 2009/22) and took stock of related work carried out in line with its guidance and recommendations. In this context, reference was made to the main outcomes of the deliberations of the core group in the past, such as the elaboration of research papers on criminalization approaches, victimization issues and public-private partnerships. Particular reference was also made to the Handbook on Identity-related Crime and contains a comprehensive guide for practitioners on international cooperation to combat specifically identity-related crime (see above in para. 2).

42. In discussing further technical assistance issues, the core group reiterated that most of the future work in this area would be contingent on the availability of resources, both to prepare technical assistance materials and actually deliver projects. The core group further agreed that joint action and synergies between the public and the private sector would be beneficial. An area that could provide a fertile ground for collaborative initiatives could be that of prevention of identity-related crime in all its forms, namely social prevention (education, awareness-raising), situational prevention (facing specific risks of victimization or training those employed to detect identity-related crime) and technical prevention (development of technical security measures to ensure the integrity of documents).

43. Furthermore, the core group agreed on the need to follow a focused approach and determine priority areas for effective interventions through technical assistance. An area of utmost significance and priority, as unanimously agreed, is that of legislative responses. In this connection, it was recognized that technical assistance would need to focus first on the development of adequate and appropriate legal frameworks to deal with identity-related crime. The objective that needs to be pursued is to assist Member States in developing new, or updating existing, offences to respond to the criminal misuse and falsification of identity, as well as putting in place the necessary legal tools and instruments to allow for effective prosecution and investigation of identity-related crime.

44. In view of the above, it was agreed that the elaboration of model legislation on identity-related crime could be of added value for Member States wishing to be guided by a set of model provisions in structuring effective legal responses. A template prepared by Prof. Gercke was brought to the attention of the core group with the aim to provide a checklist of issues that need to be considered for inclusion in a model legislation. Prof. Gercke reiterated that identity-related abuses could not be effectively criminalized per se without a unified identity management scheme. For that reason, the proposed skeleton of model legislation on identity-related crime (see appendix I) also includes aspects of a more administrative nature which are linked to the identity management agenda. Therefore Member States wishing to be guided by a model legislation based on this skeleton, may determine themselves the

scope of application of the legal framework, bearing in mind that identity management aspects may also be dealt with in the wider context of a national strategy on identity-related crime.

F. The engagement of the private sector in the development and delivery of technical assistance: Public-private partnerships

45. The representatives from the British Bankers Association (BBA) presented the work of the Association in response to financial crime, as well as their ongoing cooperation with the public sector. The BBA represents 200 financial institutions operating in 60 countries. In this framework, the BBA runs seven committees on financial crime, one of them focusing particularly on fraud. These committees are decision-making bodies and provide, for example, inputs to the government on policy matters. The BBA also channels to the government the views and concerns of the banking sector, such as on sharing, within the banking sector, information on suspicious transactions, or related to challenges arising from the increase of increased international circulation of their clients. The level of commitment of the banking sector against financial crime is illustrated by the significant budget they allow for this, by their commitment to securing their systems, and by the recruitment of qualified staff, many of them being ex law enforcement personnel.

46. The representatives from the BBA stressed the importance of private-public synergies and the cooperation of the members of the Association with law enforcement authorities, including through providing information on how to detect suspicious transactions. The BBA is, furthermore, part of the national strategy against fraud, and has taken an active part to other public-private initiatives such as awareness-raising campaigns online. Such synergies are fundamental considering the fact that financial crime is in constant evolution and requires mutual engagement of both sectors to answer adequately to these new challenges. Similarly, cooperation could be very useful in the area of money laundering as it is a major challenge encountered by the BBA members. It was noted that the inputs of the private sector in developing further the legislative and policy environment with regards to financial crime and money laundering could be valuable. The role of the international community in addressing financial crime was also stressed.

47. The BBA representatives further stressed that education of the public is a key factor. According to their experience, the systems of the banks are well protected and are not directly hacked. However, the customers' emails can be hacked and, consequently, criminals are able to get in the banking records in a typically legitimate way. They also stressed that the banking community is diverse. The investment banking and retail banking, for example, would have different interests while addressing identity-related crime.

48. In response to a question raised by Mr. Gilberto Martins de Almeida on the potential new risks arising from the increase use of new systems such as mobile phone payments, Mr. Matthew Allen stressed the need to consider the potential weaknesses of other industries, such as in retail or telecommunication sectors, while assessing the risks posed by financial crime. However, all new products do not pose the same level of risk, but the increased use of technologies such as mobile phone

payment in developing countries, for example, is a challenge. The international community could have a role as well in addressing this risk.

49. Mr. Sébastien Saillard presented the work of RESOCOM and the Reso-Club. RESOCOM specializes in the fight against identity-related crime and developed web services to check the authenticity of identification documents and passports from all countries. It was reported that over 2 million document controls were effectuated in 2011.

50. RESOCOM is a founding member of Reso-Club whose objective is to enhance exchanges and good practices between professionals of the public and private sector with regard to the fight against identity-related crime. The association Reso-Club will organize in October 2013 in Paris its Third European Forum in the Fight against Identity and Identification Document Crime. The association also endeavours to develop assistance projects for victims of identity-related crime.

51. On the basis of the above presentations, the core group discussed the elaboration of a descriptive document providing and summarizing voluntary experiences of public-private partnerships internationally, as a way of illustrating their importance. The core group authorized further action geared towards compiling cases of success in public-private partnerships to address identity-related crime in different geographical regions. A document containing a short description of each case (benefits, translated into numbers and figures) without argumentative/editorial analysis will be presented to the Commission on Crime Prevention and Criminal Justice at its twenty-second session as a Conference Room Paper.

52. The core group further authorized the Secretariat to seek more comprehensive information, including examples of practical cases, from private sector entities, represented at the meeting through BBA and Reso-Club, on the following issues: the impact of identity-related crime on those entities; the production of any quantitative (figures) and/or qualitative data, including assessments and opinions on certain ways to address the problems raised by such form of crime; the types of initiatives/measures that have been taken by the private sector entities to enhance prevention of identity-related crime; the measures that have been taken to protect customers from being victimized; the types of training available, if any, to employees and officers entrusted with a task to detect identity-related crime; the added value of strengthening public-private-partnerships to prevent and combat identity-related crime; and the fields in which synergies between state authorities and financial institutions/other private sector entities have the potential to produce tangible results and effective outcomes.

G. Presentation of indicative examples of academic projects involving aspects of prevention and detection of identity-related crime

53. The core group was briefed by Prof. Nikos Passas, supported by his colleagues in Northeastern University in Boston, U.S.A., who attended the meeting through teleconference, on a number of projects elaborated — or being under elaboration — in the university which involve aspects pertinent to the prevention and detection of identity-related crime. The first project was somewhat equivalent to undercover operation in the field of cybercrime and intended to inject data into a criminal

network to understand how the underground cyber-economy is operating. The second project, called “Mediascan”, is intended for use by banks and financial institutions and aims at detecting and tracking suspicious and irregular transactions, often involving misuse of identification information. The third project focuses on the analysis of practices pertaining to the hiding or misuse of identities in the context of informal payments and trade-based money-laundering.

H. Other matters

54. Mr. Knopjes presented the so called “Fidelity” project, a European Union project aiming at analysing shortcomings and vulnerabilities in the ePassport life cycle, and developing technical solutions and recommendations to overcome them. This 4 years project includes 19 partners (SMEs, industry, end-users, academics) and focuses on analysing the SWOT (Strength Weaknesses Opportunity Threats) during the ePassport life cycle. Mr. Knopjes reported on different issues arising at various stages of the ePassport life cycle, such as those encountered at the issuing process (security of birth certificates and other evidence of identity), or those relating to revocation and destruction of chips. Reference was made to the management of certificates, the enforcement of personal data protection throughout the process, as well as the verification of quality of biometrics data. The speaker pointed out that there was a pressing need to establish minimum international standards for birth certificates (see below) and other evidence of identity to improve the level of integrity of identity documents.

55. In addition, Mr. Knopjes made a presentation about security issues raised by breeder documents which constitute the first identification upon birth. These documents, issued under the responsibility of state authorities, often raise security issues as there are no standards or criteria established for them. The speaker stressed the absence of international standards and the lack of knowledge of other countries’ breeder documents. Currently, there is no database of such documents where state authorities could find information about the model used, and the knowledge on the issue is limited. There is a risk therefore that counterfeited breeder documents could be used to obtain valid secure id-cards or passports.

56. In the same context, Mr. Knopjes also presented a working definition of identity management as a system comprising a vision, policy and facilities for the management by state authorities of the identities of all citizens. In this regard, a table of identity infrastructure was presented to the core group, with the four phases of the cycle of the document (production, use and simultaneous control, end of use). For each of these phases, technical explanations were provided with regard to registration issues, the process followed and the expertise required.

IV. Conclusions and recommendations for future action

57. At the last session of the meeting on 18 January 2013, the Chairman of the core group summarized the main outcomes of the deliberations as follows:

(a) Elaboration of a skeleton for model legislation on identity-related crime; and

(b) Elaboration of a checklist of strategic elements in developing national strategies for the prevention, investigation, prosecution and punishment of identity-related crime.

Both outcomes are appended to the present report.

58. The Chairman further noted that the core group proposed a concrete framework of future action, specifically for the period after the completion of the sixth meeting of the core group until the twenty-third session of the Commission. In this context, the core group made recommendations on follow-up action regarding the following:

(a) Updating of a descriptive paper on the development of a framework containing the basic components of a national strategy on the prevention, investigation, prosecution and punishment of identity-related crime; and further submission of this paper to the Commission at its twenty-second session as Conference Room Paper for its consideration;

(b) Elaboration of a descriptive document compiling successful cases of public-private partnerships to address identity-related crime in different geographical regions; and further submission of this document to the Commission at its twenty-second session as Conference Room Paper for its consideration;

(c) Compilation of information on identity-related crime from private sector entities, in line with the directions and guidance mentioned above (see para. 52);

(d) Elaboration of model legislation on identity-related crime, based on the skeleton appended to this report. In terms of methodology to be followed, the initiative of the Secretariat to convene, subject to the availability of extra-budgetary funds, an ad hoc expert group to pursue this task was viewed as the most appropriate way to accomplish this task; and

(e) Seeking further information from Member States on the development and implementation of national strategies or programmes to prevent and combat identity-related crime.

Appendix I

Skeleton for model legislation on identity-related crime

1. Definition

The section could provide definitions for the most relevant terms. Apart from "identity", "means of identification", "possession", "use" and "transfer", the definition section could also contain definitions for technical terms.

2. Substantive criminal law

The model law could provide substantive criminal law provisions for online and offline identity-related crime (identity theft/identity fraud). Specific provisions or an aggravation of sentences could be provided for specific offences (e.g. falsification of access codes to military property). The model law could also provide criminal law provisions that criminalize preparatory acts such as the producing, selling, importing, exporting or possessing tools used to create false passports.

3. Procedural law

Theoretically, the model law could contain a whole set of procedural laws that would enable a country without adequate legislation on cybercrime to effectively address online identity-related crime. However, this might overlap with other initiatives and could lead to conflicts. Therefore it might be favourable to focus on solely identity-related issues. One issue, for example, could be the freezing, seizure and confiscation of assets and/or identity-related information.

4. E-evidence

Certain provisions could deal with the admissibility of specific evidence of identity-related crime. The obligation to hand out records to the victim may also be dealt with.

5. Urgent matters

The model legislation could contain provisions enabling action as a matter of urgency in on-going cases where identity-related crime is reported. One example could be "security freeze" (see above under "Procedural law").

6. Reporting and notification obligations

The model legislation could contain provisions establishing an obligation for companies which became victims of identity-related crime (with regard to customer data) to report this to law enforcement authorities. In addition, the model legislation could contain notification obligations requiring companies to notify a customer if his/her data was illegally obtained. The model legislation could also contain provisions introducing reporting mechanisms (e.g. complaint websites).

7. Protection of identity-related information

The model legislation could contain a ban on using certain identity-related information, as well as obligations to store such information by maintaining certain protection standards (e.g. encryption) and technical standards for the deletion/destruction of identity-related information.

8. Statistics

The model law could contain provisions establishing certain reporting requirements to collect statistical data for police statistics.

Appendix II

Checklist of strategic elements in developing national strategies for the prevention, investigation, prosecution and punishment of identity-related crime

This checklist summarizes the stakeholders, as well as the substantive elements and the process that each State may wish to employ in developing national strategies for the prevention, investigation, prosecution and punishment of identity-related crime.

A. Possible stakeholders or participants in a national strategy

- Public sector (public bodies responsible for id infrastructure, documents or systems, institutions responsible for policy and legislation more generally, bodies responsible for investigation and prosecution, crime prevention, etc.);
- Private sector (e.g. representatives from the financial, retail and information technologies sectors);
- Regional and international organizations.

B. Substantive elements of a national strategy

- Threat assessment — understand the nature and scope of the problem/situation;
- The gathering, dissemination and analysis of relevant information about the problem;
- Priority setting and coordination between the public and the private sector;
- Legislative elements — criminalization, law enforcement, international cooperation, as well as non-criminal/administrative measures;
- Investigative and law enforcement capacity;
- Elements to support rapid intervention to disrupt and halt ongoing identity-crime schemes;
- Crime prevention components: Social prevention (educational programmes, awareness-raising); situational prevention (information to specific groups, either because they face specific risks of victimization, or because they are employed in specific places where they are in a position to identify and stop identity-related crime); technical prevention (security measures to ensure the integrity of documents and systems);
- Victims assistance;
- Training for investigators, law enforcement and other appropriate employees and officials and the private sector;
- Cooperation between the public and private sectors in the implementation of the strategy.

C. Process in developing and maintaining a national strategy

- Commit the necessary resources for implementation;

- Initial consultations at all levels within the governmental sector, and with the private sector;
- Ongoing mechanisms for vertical coordination (particularly in federal States);
- Consultation or coordination with international stakeholders, where appropriate;
- Secure ongoing consultations among stakeholders;
- Review the success and sustainability of the implementation of the strategy.