United Nations TD/B/C.II/EM.5/3

United Nations Conference on Trade and Development

Distr.: General
10 April 2015

Original: English

Trade and Development Board
Investment, Enterprise and Development Commission
Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned
Geneva, 25–27 March 2015

Report of the Multi-year Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned

Held at the Palais des Nations, Geneva, from 25 to 27 March 2015

Contents

Page

I. Chair's summary 2
A. Opening statements 2
B. Trends and legal challenges in e-commerce 2
C. E-transaction laws 3
D. Protecting consumers online 4
E. Data protection and cybercrime 6
F. Best practices of regional cyberlaw development 8
G. The way forward 9
II. Organizational matters 12
A. Election of officers 12
B. Adoption of the agenda and organization of work 12
C. Outcome of the session 12
D. Adoption of the report of the meeting 12

Annex

Attendance 13

Introduction

1. The Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned, was held at the Palais des Nations in Geneva from 25 to 27 March 2015, as agreed by the Trade and Development Board at its fifty-ninth executive session on 24 June 2014. Over 200 participants representing all stakeholder groups attended the meeting.

I. Chair's summary

2. The expert meeting explored the following key issues: how to assess needs for cyberlegislation, best practices in fostering cross-border online transactions and improving security online, the role of stakeholders, actions that can be taken to monitor progress in developing countries and regions in developing relevant cyberlegislation and how assistance from international organizations and other development partners can help facilitate the enforcement of compatible e-commerce laws.

A. Opening statements

3. The Director of the Division on Technology and Logistics of UNCTAD highlighted the rapid expansion and evolution of e-commerce among developed and developing countries. E-commerce had a transformational impact on the global economy, and recent trends had shown its effect on global supply chains. It offered both opportunities and challenges, making adequate policy responses particularly important. More work was needed, however, to ensure an enabling environment for e-commerce that was inclusive and facilitated economic growth and sustainable development.

4. Since the release of its first landmark report on e-commerce in 2000, until the publication in 2015 of the *Information Economy Report 2015*,[1] UNCTAD had played a leading role in that field. In addition, it worked closely with other international organizations in the area of e-commerce and information and communications technology (ICT) for development.

5. The Chief of the ICT Analysis Section of the Division on Technology and Logistics provided an overview of the work programme of the meeting, highlighting key trends in e-commerce and critical issues concerning the creation of a legal and regulatory environment conducive to inclusive e-commerce. Drawing attention to the global mapping of cyberlaws that had been undertaken by the UNCTAD secretariat, he said that there was still progress to be made by developing countries in adopting relevant laws.

B. Trends and legal challenges in e-commerce

6. Panellists highlighted the rapid rise and geographic expansion of e-commerce, which was expected to continue in coming years. The widespread improvement of ICT had brought about accelerated online demand for e-commerce services and delivery. E-commerce had enabled more small and medium-sized enterprises to engage in exports and to export to more countries than offline commerce. Emerging markets and developing countries were gaining significance, both as consumers and suppliers online. To make

[1] UNCTAD, 2015, *Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries* (New York and Geneva, Sales No. E.15.II.D.1, United Nations publication).

e-commerce available globally, it was important to work towards greater harmonization and transparency. The panellists raised concerns about consumer protection, privacy and data protection and cybercrime. This led to a discussion stressing the need to invest in digital infrastructure and to put in place cyberlaws and regulations as a means of promoting trust and security online.

7. There were several challenges to be met, such as the need to invest in human capital to make e-commerce businesses effective and efficient. Further, public education and awareness-raising efforts were needed so that the public could benefit more from e-commerce. One panellist underscored the need to create an e-commerce environment where aspiring online businesses could flourish. Building local human capacity was important, especially among mid-level managers, to strengthen local e-commerce businesses and ensure that they were run effectively. Infrastructure development posed another challenge in many countries. In the view of some panellists, road transport was crucial for facilitating goods delivery into and within countries. Secure payment solutions were also essential, and the 660,000 post offices around the world could play a central role in e-commerce.

8. It was important to cultivate a legal framework for e-commerce that maintained a balance between regulation, competition and innovation. Furthermore, legal frameworks had to be supported by well-resourced institutions with skilled staff to allow e-commerce to be conducted in a secure, legal and efficient manner. Complications could arise from different and inconsistent national schemes, for example related to taxation, and it was necessary to ensure interoperability and compatibility of national e-commerce networks, systems and legal environments. Appropriate legal frameworks and law enforcement agencies should serve to promote individual rights, prevent harm and facilitate commercial transactions in e-commerce. At the same time, there were costs involved in adopting and enforcing cyberlaws. For example, in the European Union, the cost to businesses of complying with data protection laws had been estimated at about EUR 2 billion annually.

9. In the view of some experts, e-commerce should be integrated in broader development strategies. E-commerce and cybersecurity should not only be considered from a legal and business perspective, but should also take into account economic and social development objectives. Social inclusion and universal access to e-commerce services for all citizens were also important factors to be borne in mind. Some experts called upon UNCTAD and other international organizations to assist Governments in strengthening their national e-commerce ecosystems, markets and cyberlaws to support broader economic development.

C. E-transaction laws

10. In an informal session devoted to the development of e-transaction laws and related legal issues aimed at facilitating e-commerce, participants considered the need for compatibility of laws to facilitate cross-border trade and discussed variations in domestic public and private law across and within regions. The United Nations Convention on the Use of Electronic Communications in International Contracts (2005) was an example of a recent international legal instrument relating to e-commerce.

11. Electronic identification and issues such as authentication had long posed a challenge for the implementation of e-transactions, hampering cross-border e-commerce. The European Union had made headway by adopting Regulation No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/European Commission, making mutual recognition of electronic identification mandatory. A number of experts expressed interest in the applicability of this resolution for cross-border trade between the European Union

and other countries. A representative of the European Commission stated that such an approach could be considered under certain conditions, including respect for non-discrimination and technology neutrality.

12. Care should be taken to ensure that the national implementation of e-transaction laws did not inadvertently hinder cross-border trade. The use of public key infrastructure for signatures could at times be an obstacle to cross-border recognition of electronic signatures. Several experts highlighted the importance of technology neutrality, one of the principles advocated by the United Nations Commission on International Trade Law. Cross-border interoperability in the recognition of signatures was crucial to fostering international trade. Single windows for paperless trade were also useful.

13. There were some opportunities for developing countries to leapfrog developed countries grappling with legacy systems with regard to e-transactions, as well as other e-commerce-related areas such as infrastructure. Experts discussed various approaches to harmonizing e-transaction laws, ranging from the establishment of international standards – on authentication, for example – to that of a treaty. There was consensus that e-transaction measures should be tailored to the particular conditions and circumstances of each country. Other issues included the role of intermediaries, the lack of national capacity in the implementation of e-transaction laws, and cases where regulation was considered to be a more appropriate course of action than the enactment of a law.

14. There had been rapid growth in innovative retail payment instruments for electronic transactions. Emerging payment methods ranged from mobile payments to pre-paid telephone cards. Many of the new instruments had improved the access of the unbanked population to electronic payments and were valuable tools for financial inclusion, even in rural areas. With the burgeoning of innovative retail payment instruments, however, new risks needed to be addressed. Risks existed in the key phases of the electronic payment process: pre-transaction, authorization, clearing, settlement and post-transaction. There were technological risks to be addressed as well. Meeting these needs required a holistic approach that took into account developments in technology and in financial systems.

15. Innovation in the financial services sector had helped some developing countries to achieve greater financial inclusion. Kenya had been a pioneer in this regard, notably by allowing the expansion of mobile payments. The Central Bank’s granting of authorization to a mobile company to transfer money in 2006 had significantly shifted the payments system structure away from large value payments to the mobile payment platform.

16. Experts shared national experiences and raised questions about the complexity of the issue, especially concerns among central banks about granting banking licences to mobile operators. It was important to strike a balance between fostering innovation and protecting the users. In general, consumers were considered to be best protected in markets characterized by effective competition. Some experts argued against making the distinction between telecommunications-led and bank-led mobile money systems. The key concern should be whether a provider of the payment service was able to carry through efficiently. Meanwhile, the convergence between the communications industry and the banking industry called for close collaboration between regulators of the two domains.

D. Protecting consumers online

17. In another informal session, experts discussed the concerns of online consumers, including in the case of cross-border e-commerce. They also considered relevant legislation and approaches to ensure that consumers received equal protection both offline and online.

18. Panellists noted that e-commerce, both domestic and cross-border, was expanding owing to the increased reliance on the Internet and the availability of mobile devices around

the world. Wherever Internet access was widespread, the nature, channel and timing of consumer transactions and interactions were fundamentally transformed. Technology was progressing quickly, and the new challenges that were arising as a result had to be addressed. Many countries still lacked specific rules for protecting consumers online.

19. While e-commerce presented benefits and advantages for consumers (greater choice, convenience), it also raised concerns about fraud, spam, privacy, data security and information security. Consumers were faced with digital risks and costs associated with hidden fees, delivery and fulfilment, data exploitation and privacy, opaque terms and conditions, market structure and quality of services. A distinction could be made between consumer protection issues related to the payments involved and those related to the delivery and quality of the goods and services ordered online. Cross-border e-commerce was particularly challenging because of different legal principles across borders and the lack of cross-border dispute resolution mechanisms. At the same time, some experts cautioned that overly strong consumer protection could constitute a barrier to trade.

20. Consumers' vulnerability online should be taken into account when preparing laws. An additional challenge lay in the many areas of law involved – civil, criminal, intellectual property, consumer protection – as well as in the diverse regulatory bodies. In the event of a dispute, consumers needed simple, effective redress mechanisms, without having to resort to litigation, especially in the case of low-value transactions common to business-to-consumer commerce (B2C).

21. Panellists discussed ways to build the confidence of consumers online. These included legal and technical measures as well as increased cooperation among consumer protection agencies. An important first step was to adopt consumer protection laws. At the international level, the United Nations was currently revising the guidelines for consumer protection. In this context, Member States had agreed to discuss e-commerce, building on the Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) drawn up by the Organization for Economic Cooperation and Development; these were also under revision. The revision would reflect the increased access to mobile devices (1.7 billion devices connected to the Internet), where consumers, including children, enjoyed better access to mobile and online payment tools, digital content products and participative e-commerce. The Guidelines contained several principles, such as transparent and effective consumer protection no less than that afforded in other forms of commerce; fair business advertising and marketing practices; and clear and transparent information disclosure online.

22. Beyond the adoption of laws at the national level, it was essential to strengthen the regulatory agencies. Moreover, it was necessary to increase cross-border interoperability of systems proposing the same rules – and convergence of different technology platforms – such as the legal characterization of products across borders and codes of conduct in cross-border transactions. International cooperation should also be encouraged to combat cyberfraud and unfair e-commerce practices.

23. Suggestions on how to improve domestic laws and strengthen the capacities of consumer protection agencies included greater inter-agency cooperation, training of national agencies in developed and developing countries, cooperation agreements among consumer protection agencies, the creation of a pool of national experts, more effective exchanges of information, and opportunities for intergovernmental debate in forums such as UNCTAD. Networks, such as the Global Privacy Enforcement Network, the International Competition Network and the International Consumer Protection and Enforcement Network; educational campaigns; and possibilities for consumers to file complaints online were cited as useful mechanisms.

24. Industry self-regulation should be further encouraged and accompanied by effective enforcement. Solutions might also include stronger protection of consumers by payment intermediaries, such as credit card companies. Some experts recommended that Government work with companies to ensure that similar protection was available for all means of payment. Greater transparency concerning data breaches was also important.

25. In the eyes of some experts, there was a need to increase the penalties for economic fraud, as the risks for people engaging in such activities were currently too low. Furthermore, to improve the overall environment in which consumers were evolving, the following factors should be considered: secure payment methods; greater transparency on what type of fraud, identity theft and other crimes were committed; access to effective inexpensive online redress platforms; consumer education and infrastructure neutrality.

E. Data protection and cybercrime

26. Experts explored how legal and regulatory frameworks for protecting personal data and privacy could enhance trust in the use of the Internet and combat cybercrime. UNCTAD had conducted a mapping exercise that had found that 107 countries, including 51 developing countries, had in place data protection and privacy legislation, while 117 countries, of which 82 were developing and transition economies, had enacted cybercrime laws.

27. One of the main challenges in developing cyberlegislation was to strike a balance between data protection, and ease of data flow and freedom of information. There were new complex issues to contend with, including some alleged outsourcing of security functions aimed at circumventing data privacy restrictions in certain jurisdictions. The rising importance of cloud computing, whose impacts on data privacy and protection had been examined in the *Information Economy Report 2013*,[2] had compounded the problem.

28. Data protection laws were sorely needed in many developing countries. To ensure data protection, cybersecurity measures should adhere to the "do no harm" principle. One panellist proposed that Government and private sector stakeholders should apply the principle to achieve a just balance between government surveillance of data for cybersecurity reasons and data privacy. Cybersecurity measures, including surveillance, should be taken only if necessary, proportionate, and narrowly focused. They should also apply equally to all individuals and legal entities. The application of the principle would rekindle trust in national security, law enforcement and the private sector. The incorporation of the tests of necessity, proportionality and narrow focus in international cybersecurity agreements could help bring clarity and harmonization, and enhance cross-border cooperation.

29. Without such safeguards, countries risked defeating the purpose of cybersecurity by undermining encryption standards, exploiting back-door vulnerabilities in infrastructure and applications, and even releasing malware. Some positive initiatives to enhance cybersecurity were already under way, in the form of public–private partnerships and the harmonization of legal instruments. There was also an opportunity to enhance cybersecurity through better regulation of intermediaries.

30. One expert noted that business organizations were increasingly falling victim to cybercrime. Cross-border cybercrime affected international trade and was difficult to investigate and prosecute. The United Nations Office on Drugs and Crime (UNODC) cybercrime repository had recently been set up to enhance international cooperation on

[2] UNTAD, 2013, *Information Economy Report 2013: The Cloud Economy and Developing Countries* (New York and Geneva, Sales No. E.13.II.D.6, United Nations publication).

cybercrime by compiling case law and lessons learned relevant to data protection. Several participants welcomed the repository as a useful reference for law enforcement, especially in developing countries. Its usefulness would partly depend on international collaboration, as the database contained information volunteered by countries.

31. Some experts called for more enhanced international cooperation. Regional cooperation had so far been more effective than international cooperation. Current mechanisms were not functioning effectively, and stakeholders were not fully aware of the relevance of international cooperation. Informal and formal mechanisms could be used to strengthen such cooperation. While cyberthreats were increasingly complex and evolving rapidly, the international community had not acted on the threats, and cybercriminals were exploiting differences between jurisdictions. There was scope for greater harmonization of data protection regimes. To achieve credible cooperation in data protection, a more altruistic approach serving the common good might be necessary. In an interconnected world, cybersecurity could not be ensured in any single country if others were at risk.

32. Identity and data theft, phishing, hacking of personal e-mail accounts and cyberfraud undermined the adoption of e-commerce and consumer trust in digital finance and mobile money. While some African Governments had put in place cybersecurity policies, data protection and electronic transaction legislation, and had set up computer emergency response teams, they faced significant implementation obstacles. These included a limited understanding of cybercrime and ineffective coordination among stakeholders and enforcement. In addition, cybercrime was increasingly linked to other transnational crimes, such as terrorism, human trafficking and money laundering. Other countries provided for extraterritorial jurisdiction in cases of cybercrime, but had in practice been unable to obtain electronic evidence from outside its national borders. Some experts called on international organizations to help define common legal principles for dealing with related challenges. One participant said that the Electronic Evidence Guide, developed by the Council of Europe for police officers, prosecutors and judges, was available to all countries as a reference.

33. Several experts recognized the difficulty of investigating and prosecuting cybercrimes. Some noted that law enforcement agencies needed more training to deal with cybercrime and appealed to relevant international organizations to consider this when supporting e-commerce and law reform. To strengthen enforcement, the UNODC cybercrime repository would benefit from contributions from multiple stakeholders to improve its scope and coverage. To this end, UNODC was encouraged to increase its presence in multi-stakeholder meetings that discussed cyberlaw and cybersecurity. One expert proposed that producers of technology and decision-makers in technology standards had a responsibility in preventing the criminal use of their technology. Where critical ICT infrastructure was privately owned, Governments faced an additional challenge in ensuring its safety. The private sector had a level of responsibility that could be defined in the context of public-private partnerships. Such partnerships were particularly important when countries set up computer emergency response teams.

34. One panellist said that the next phase of e-commerce would increasingly be characterized by seamless interactive communication between users, devices (the Internet of Things) and services. Trust online would then become even more crucial, and stakeholders would need to adjust their behaviour in order to respond to the increased exchange of data. Access to personal data by multiple devices and applications resulted fragmented identification management and limited control over data exchange protocols by consumers. Greater dependency on online services and increased monetization of personal data would require greater attention to data protection and control by multiple stakeholders – Government, citizens, consumers, employers and service providers. Fragmentation was

also due to people and products having multiple identities online. Further research was needed on how to link digital identity to offline identity.

35. To build the trust of online consumers, it was necessary for them to know the value and tradability of their data, and to understand how their data were managed. They also needed to be aware of the means at their disposal to enforce data protection. Increased awareness would result in less vulnerability to cybercrime and in consumers actively being able to claim their privacy. Eventually, users might also share in the value of their personal information.

36. Several experts called upon the international community to continue raising awareness among stakeholders of the impact of cybercrime, including its link to other types of crime. Well-informed stakeholders were better equipped and empowered to make decisions about the data they divulged and how to protect such data. International cooperation on cybersecurity also needed to improve, including through the harmonization of data protection regimes. Currently, few international forums were available to discuss these issues. UNCTAD could offer a platform for discussions on data protection and privacy online.

F. Best practices of regional cyberlaw development

37. Participants examined the efforts of various regional groupings, UNCTAD and other partners to achieve law reform. They discussed the key challenges involved in implementing compatible laws, best practices and cross-regional lessons learned.

38. Through its work in several regions, UNCTAD had identified the following challenges to regional harmonization:

(a) Cross-country differences in terms of legislation, capacity, resources and political situation;

(b) Different legal regimes, for example civil or common law;

(c) Different approaches to the adoption of regional agreements; hard versus soft approach;

(d) Various approaches to the national adoption and implementation of law.

39. The region of the Association of Southeast Asian Nations faced challenges in key areas with regard to e-commerce. These included limited broadband speed and the high costs of broadband use; inadequate e-payment penetration and bankability, despite innovations; inefficient logistics and customs handling; lack of trust and confidence in the Internet, partly due to high levels of cybercrime; uncertainty regarding dispute resolution; and the lack of a regional body to champion e-commerce at the regional level.

40. In the case of the East African Community (EAC), cyberlaws needed to be complemented by an enabling environment, including proper ICT infrastructure. The EAC Council of Ministers had approved the development of a regional framework for cyberlaws. To this end, the EAC, with the assistance of UNCTAD, had set up a task force which comprised a cross-section of stakeholders, including Government, the legislature, the judiciary and the private sector. Two frameworks had been adopted using a soft approach. The major challenge was the uneven pace of national implementation of cyberlaw frameworks. There was a need to involve the right people at the right time – namely the political class at the beginning for general direction, and technocrats for the process of development. Other important needs were capacity-building, sharing experiences, continuous monitoring of case law and further international cooperation.

41. Several panellists reiterated the importance of an enabling environment for e-commerce to thrive. In the Economic Community of West African States (ECOWAS), major challenges had been limited resources and the inability of countries to respect deadlines set by the ECOWAS Commission. To improve e-commerce, it was important to raise consumer confidence in online transactions.

42. The Arab region lagged behind developed countries in the adoption and enforcement of cyberlegislation. There was a need to develop a standardized reference for regulatory and legal issues related to cyberspace, harmonize cyberlaws and terminologies, and clearly define the roles and responsibilities of various institutions. Further, there was scope for more collaboration within countries for the adoption of laws. Similarly, law enforcement was a challenge, as was the absence of procedural decisions and regulatory instruments. In some cases, electronic documents were not fully recognized.

43. Based on best practices observed in the various regions, there was a need at the national and regional levels for a strong political commitment to strengthening cyberlaws. Effective collaboration between regulatory and statutory authorities at both levels was crucial to adopt and enforce legislation. This could be facilitated by setting up an intergovernmental coordination committee. Dialogue between the public and private sectors was equally relevant. Furthermore, efforts should be made to raise awareness of the cyberlaw reform process.

44. In order to keep the momentum for cyberlaw reform, Government needed to create comprehensive road maps, detailing milestones and timelines, thus facilitating monitoring and reporting of developments to regional institutions, donors and international organizations.

45. Several experts emphasized the need for capacity-building, while others suggested that technical workshops should be complemented by meetings on e-commerce and cyberlaws to heighten political awareness of the issues. Such initiatives could help foster political will and link e-commerce with sustainable development.

46. Several experts said that they would welcome the organization by UNCTAD of similar meetings to discuss e-commerce and cyberlaws. Such gatherings should involve a wider representation of stakeholders. Several experts recalled that e-commerce legislation was only one of several important pillars of e-commerce.

47. The UNCTAD secretariat drew attention to the need for developing better statistics and encouraged member States to include e-commerce-related questions in their official statistical surveys. Some experts proposed the development of an UNCTAD repository of tools, programmes and studies currently being offered by various organizations in the area of e-commerce. One expert recommended that cyberlaws be included in university curricula, possibly developed with the assistance of international organizations such as UNCTAD.

G. The way forward

48. In the final informal session, experts discussed how different stakeholders could support the strengthening of cyberlaws for international e-commerce in developing countries.

49. While cyberlaws might help establish legal certainty, foster trust, encourage best practices and ensure legal redress, they were unable to develop technology or to be innovative. Legislation alone would not encourage e-commerce or generate cross-border trade. It could prevent discriminatory practices, but could not ensure inclusion or affect the distribution of e-commerce benefits. Cyberlaw should be technology neutral and thus

flexible to adapt to new innovations. It should be an enabler, not a barrier to trade, and should provide a framework, apply principles of interoperability and embody good practices.

50. As the world's largest B2C e-commerce market, China's experience with preparing its legal framework and broader policies for e-commerce was valuable. China's market demand and the speed of development had outpaced policy, and the country faced challenges in the regulation of service providers, consumer protection and transactions with other jurisdictions. Its draft e-commerce law was expected to be approved by 2018. The Government had set up an action plan called Internet Plus and strategic guidelines to help the Chinese market better respond to and integrate new technological developments, such as mobile Internet, cloud computing, big data and the Internet of Things. Legislation would be supported by current measures to build consumer confidence and capacities of small and medium-sized enterprises to engage in e-commerce, including in rural areas. The goal was to boost domestic and international e-commerce by encouraging local entrepreneurship and innovation.

51. In the case of Uganda, the country had taken nearly a decade to prepare the legal ground for e-commerce legislation, which had been enacted in 2011. However, effective implementation had yet to be achieved. One obstacle had been limited appreciation and understanding of the cyberlaw frameworks by policymakers, law enforcement bodies and civil society. This had made consultation and consensus on legal instruments difficult. The Government of Uganda had sought assistance, including from UNCTAD, in building the capacity of stakeholders and ensuring that trainees became multipliers of that knowledge. The Government had also set up a multi-sectorial think-tank team responsible for advising on the implementation of cyberlaws, including a public awareness strategy. Awareness-raising had been carried out through physical visits to stakeholder groups such as bankers, insurers, judges, law enforcement officers, law practitioners and traders, who learned about different technical and legal issues where their cooperation was needed for cyberlaw implementation.

52. Experts noted overlaps between cyberlaw and international trade law in the area of e-commerce. While there was a general understanding that e-commerce fell within the purview of World Trade Organization (WTO) agreements, the ability of WTO to build on that understanding had been limited. In principle, since the delivery of services was technology neutral, the same conditions applying to general services agreements should apply to electronic delivery services. However, no officially agreed classifications and definitions related to international trade in ICT services, and ICT-enabled services had yet been established; a provisional moratorium on duties for electronic transmissions had been in place since 1998. Current WTO agreements for trade in services could offer a solid framework of principles and obligations that reflected good governance for online trade. While WTO agreements had binding obligations, the Organization did not prescribe how obligations should be implemented. UNCTAD could offer a useful complementary platform for future exchanges of good practices in this regard.

53. Although cyberthreats affected all regions, Africa was especially vulnerable. The lack of secure and reliable electronic infrastructure and cyberlaws contributed to its exclusion from the knowledge economy. While cyberlaw harmonization was well advanced in some subregions, others had not yet conducted such an exercise, and many ICT sector activities remained unregulated. The recent African Union Convention on Cybersecurity and Personal Data Protection (2014) was a significant advancement, albeit not yet in force, pending ratification by 15 countries. A qualitative approach to create a trustworthy legal framework required proactive digital risk management, effective implementation of cyberlegislation, evaluation and monitoring mechanisms, and continuous improvement of the enabling environment. The latter involved the acceleration of the entry into force of the

Convention, and the transposition of its provisions into national legislation. In addition to legislative texts on data protection, one expert proposed that a commission be set up to monitor its implementation. Finally, capacity-building of all stakeholders was essential.

54. Several experts agreed that e-commerce was key to fostering inclusive economic development, and while existing model laws, such as those developed by UNCITRAL, were relevant, more work was needed in designing model laws or guiding tools in specific areas, such as legal redress, anti-spam provisions, the responsibilities of service providers, taxation of online transactions, and cloud computing. More research was also necessary on the impact of cyberlaws on consumers and practitioners. In addition, some experts suggested that the role of non-State actors be further explored, because critical infrastructure and information were increasingly in private hands. The private sector and intermediaries, academia, non-governmental organizations and other players should be included in future discussions on cyberlegislation.

55. Some participants said that adequate cyberlaws were necessary but insufficient for e-commerce development in developing countries. The *Information Economy Report 2015* had proposed a holistic approach to developing a national e-commerce strategy based on a framework assessing eight key policy areas. The UNCTAD secretariat informed experts that the Organization could provide assistance to countries in developing a national e-commerce strategy through its ICT Policy Review Programme. UNCTAD could also offer capacity-building and training in statistics, including in information economy statistics. Moreover, the Automated System for Customs Data Programme, commonly known by its acronym ASYCUDA, could help address trade facilitation through customs automation, and an UNCTAD training programme on e-commerce for practitioners was also available.

56. International organizations could play an important role by, among other things, building sustainable capacity for cyberlaw in developing countries, including by providing advisory services in the long process of drafting, adopting and enacting cyberlegislation. The international community could also foster dialogue between stakeholders and help build networks. Some experts requested that UNCTAD set up an online discussion on cyberlaw for e-commerce to ensure that cyberlaw reform was better reflected in political agendas.

57. Several experts recalled that it would be important to link the 10-year review of the World Summit on the Information Society (WSIS) to the discussions on the proposed sustainable development goals, to ensure that future economic growth, including through e-commerce, was coherent with sustainable development and social inclusion.

58. In conclusion, experts stressed that cyberlaw adoption should be an enabler of e-commerce, not a barrier to cross-border trade. As legislation did not guarantee effective implementation, it should be complemented by other efforts to create an enabling environment. Many developing countries, especially in Africa, needed to build the capacity of all stakeholders in order to draft, adopt, implement and monitor cyberlaws, as well as to ensure they were in line with regional and international conventions on cybersecurity and electronic transactions. Knowledge transfers were needed to make countries more autonomous in their capacity to uphold laws. Future work on cyberlaws to unlock the potential of e-commerce for developing countries should aim at an inclusive information economy. The work should be carried out in the context of the sustainable development goals beyond 2015 and of the WSIS review and its follow-up. Finally, UNCTAD should continue to offer a platform for ongoing discussions and the exchange of best practices on matters related to cyberlaw.

II. Organizational matters

A. Election of officers

(Agenda item 1)

59. At its opening plenary, on 25 March 2015, the expert meeting elected Mr. Timo Kotilainen (Finland) as its Chair and Mr. Humberto Jiménez as its Vice-Chair-cum-Rapporteur.

B. Adoption of the agenda and organization of work

(Agenda item 2)

60. Also at its opening plenary, the expert meeting adopted the provisional agenda contained in TD/B/C.II/EM.5/1.

C. Outcome of the session

61. At its closing plenary on 27 March 2015, the multi-year expert meeting agreed that the Chair should provide a summary of the discussions.

D. Adoption of the report of the meeting

(Agenda item 4)

62. At its closing plenary, the multi-year expert meeting authorized the Vice-Chair-cum-Rapporteur, under the authority of the Chair, to finalize the report after the conclusion of the meeting.

Annex

Attendance*

1. Representatives of the following States members of UNCTAD attended the expert meeting:

Afghanistan
Algeria
Angola
Argentina
Belgium
Benin
Bhutan
Brazil
Burkina Faso
Burundi
Cabo Verde
Cameroon
Canada
China
Côte d'Ivoire
Cuba
Czech Republic
Democratic Republic of the Congo
Dominican Republic
Ecuador
Egypt
Ethiopia
Finland
France
Gambia
Germany
Ghana
Guatemala
Guinea
Guinea-Bissau
Hungary
India
Indonesia
Japan
Jordan
Kenya
Latvia
Lesotho
Liberia
Libya
Madagascar
Mali
Mauritania
Mauritius
Mexico
Montenegro
Namibia
Niger
Nigeria
Oman
Panama
Paraguay
Philippines
Portugal
Qatar
Saudi Arabia
Senegal
Sierra Leone
Spain
Sudan
Switzerland
Thailand
Togo
Trinidad and Tobago
Tunisia
Turkey
Uganda
United Arab Emirates
United Republic of Tanzania
United States of America
Zambia
Zimbabwe

* This list contains registered participants. For the list of participants, see TD/B/C.II/EM.5/INF.1.

2. The following intergovernmental organizations were represented at the session:

African, Caribbean and Pacific Group of States
Economic Community of West African States
European Union
Organization for Economic Cooperation and Development
Organisation Internationale de la Francophonie
Organization of Petroleum Exporting Countries Fund for International Development

3. The following United Nations organs, bodies or programmes were represented at the session:

International Trade Centre
Internet Governance Forum
United Nations Commission on International Trade Law

4. The following specialized agencies and related organizations were represented at the session:

International Telecommunication Union
Universal Postal Union
World Bank
World Trade Organization

5. The following non-governmental organizations were represented at the session:

General category

Consumers International
International Network for Standardization of Higher Education Degrees
Village Suisse ONG

United Nations TD/B/C.II/EM.5/3/Corr.1

United Nations Conference on Trade and Development

Distr.: General
22 April 2015

English only

Trade and Development Board
Investment, Enterprise and Development Commission
Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned
Geneva, 25–27 March 2015

Report of the Multi-year Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned

Held at the Palais des Nations, Geneva, from 25 to 27 March 2015

Corrigendum

Title

The title should read: Report of the Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned

GE.15-08109 (E)
1508109