United Nations A/74/130

General Assembly

Distr.: General
30 July 2019

Original: English

Seventy-fourth session
Item 109 of the provisional agenda*
Countering the use of information and communications technologies for criminal purposes

Countering the use of information and communications technologies for criminal purposes

Report of the Secretary-General

Summary

The present report has been prepared pursuant to General Assembly resolution 73/187, entitled "Countering the use of information and communications technologies for criminal purposes". In that resolution, the General Assembly requested the Secretary-General to seek the views of Member States on the challenges that they faced in countering the use of information and communications technologies for criminal purposes and to present a report based on those views for consideration by the General Assembly at its seventy-fourth session.

The report contains information on the views of Member States submitted pursuant to the aforementioned resolution.

* A/74/150.

Contents

		Page
I.	Introduction	4
II.	Replies received from Governments	4
	Argentina	4
	Armenia	6
	Australia	8
	Austria	10
	Belarus	11
	Bolivia (Plurinational State of)	12
	Botswana	14
	Brazil	15
	Canada	16
	China	18
	Colombia	19
	Costa Rica	20
	Czechia	22
	Democratic People’s Republic of Korea	23
	El Salvador	23
	Estonia	24
	France	25
	Georgia	26
	Germany	27
	Ghana	28
	Hungary	28
	India	30
	Iran (Islamic Republic of)	32
	Iraq	33
	Ireland	35
	Israel	36
	Italy	36
	Japan	37
	Jordan	39
	Lebanon	39
	Liechtenstein	41
	Malaysia	41
	Mongolia	43
	Morocco	44
	Myanmar	46

Netherlands 48
New Zealand 49
Nicaragua 51
Norway 51
Peru 52
Philippines 53
Portugal 55
Qatar 57
Romania 57
Russian Federation 59
Saudi Arabia 60
Serbia 61
Singapore 63
Slovakia 64
Slovenia 66
South Africa 66
Spain 68
Sri Lanka 70
Switzerland 71
Syrian Arab Republic 72
Tajikistan 74
Thailand 74
Turkey 76
United Kingdom of Great Britain and Northern Ireland 77
United States of America 79
Venezuela (Bolivarian Republic of) 81

I. Introduction

1. In its resolution 73/187, entitled “Countering the use of information and communications technologies for criminal purposes”, the General Assembly requested the Secretary-General to seek the views of Member States on the challenges that they faced in countering the use of information and communications technologies for criminal purposes and to present a report based on those views for consideration by the General Assembly at its seventy-fourth session.

2. Pursuant to that request, in notes verbales CU 2019/55/DTA/OCB/CMLS and CU 2019/90/DTA/OCB/CSS, dated 13 February 2019 and 19 March 2019 respectively, and issued by the United Nations Office on Drugs and Crime (UNODC), the Secretariat invited Member States to submit information on the challenges they faced in countering the use of information and communications technologies for criminal purposes. The Secretariat informed Member States that the information would be used to prepare the report on the implementation of resolution 73/187, to be presented to the General Assembly for consideration at its seventy-fourth session. The Secretariat noted that national submissions for the purposes of the report should not exceed 1,000 words, excluding the text of any laws or legislation that the Member State might wish to submit. Laws and/or legislation appended to the submission would be made available on the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal as an additional information resource.

3. In response to the invitation, the following Member States provided their views: Argentina, Armenia, Australia, Austria, Belarus, Bolivia (Plurinational State of), Botswana, Brazil, Canada, China, Colombia, Costa Rica, Czechia, Democratic People’s Republic of Korea, El Salvador, Estonia, France, Georgia, Germany, Ghana, Hungary, India, Iran (Islamic Republic of), Iraq, Ireland, Israel, Italy, Japan, Jordan, Lebanon, Liechtenstein, Malaysia, Mongolia, Morocco, Myanmar, Netherlands, New Zealand, Nicaragua, Norway, Peru, Philippines, Portugal, Qatar, Romania, Russian Federation, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Switzerland, Syrian Arab Republic, Tajikistan, Thailand, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America and Venezuela (Bolivarian Republic of).

4. Those views are reflected in the summaries prepared by the Secretariat that are presented below. The submissions covered challenges at both the national level and the international level, as well as actions taken to address them at both levels, including in the framework of existing specialized mechanisms. Member States provided information on technical and technology-related challenges and shared their experiences in tackling them. They also highlighted the importance of international cooperation in countering the use of information and communications technologies for criminal purposes.

II. Replies received from Governments

Argentina

5. Argentina noted that the greatest challenges that States faced in countering the use of information and communications technologies for criminal purposes included:

(a) The scope of international instruments. With the exception of the Council of Europe Convention on Cybercrime, other international agreements on the subject have not yet been adopted. Argentina is actively contributing to the activities of the Council of Europe Cybercrime Convention Committee and recommends that States that are not yet parties to that Convention consider acceding to it in order to strengthen the implementation of it and enhance adherence to it by countries that are not members of the Council of Europe. However, taking into account the global nature of the phenomenon of cybercrime and the need to have in place mechanisms to respond to it globally, Argentina supports both the processes within the framework of the

Council of Europe Convention and the discussions that seek to advance, within the framework of the United Nations, towards the negotiation of a universal legal framework on the matter;

(b) Difficulties for cross-border access to digital evidence. The main difficulty encountered in most cases is that the data that constitute evidence are located in a jurisdiction different from the one in which the criminal proceeding is carried out and, in almost all cases, are in the possession of private companies. The solutions proposed so far to these problems, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act of the United States (in force) and the e-evidence initiative of the European Union (in process), do not fully address the needs of third countries;

(c) Insufficient capacity to measure results in the exchange of information and good practices. In many cases, it is difficult to measure results in terms of exchange of good practices and information set forth in agreements;

(d) Difficulties in updating the regulatory framework in relation to technological progress. Keeping the criminal regulatory framework up to date, in terms of both substance and procedure, entails many difficulties, which are more serious in countries with codified legal systems;

(e) Low levels of awareness among the population and in organizations. An essential aspect of the fight against crime is that related to prevention. In cybercrime, prevention is directly linked to awareness-raising, among people and organizations, about the risks and threats that the use of information and communications technologies entails. It is necessary to formulate national awareness plans under which efforts and initiatives, both private and public, are articulated in a way that ensures coherence and optimizes the use of resources;

(f) Responsibility of the private sector. The private sector plays a fundamental role in relation to the challenges posed by cybercrime. The responsibility of companies involves aspects such as the control and management of data vulnerabilities presented by platforms and devices and the use of social networks for criminal purposes. Beyond the voluntary cooperation of the private sector, it is necessary to analyse the need for mandatory compliance rules;

(g) Increasing risks. The profusion of the use of relatively low-cost “smart” devices that allow access to the Internet without a minimum level of security increases the grounds for potential attacks and the scope of cybercrime. To address this challenge requires complementary State policies and corporate responsibility strategies. State-driven projects aimed at enabling mechanisms for decrypting information from devices and/or applications, as well as backdoor mechanisms, entail a risk. The tools for information penetration and information extraction or monitoring proposed by various judicial bodies also require evaluation.

6. Argentina identified the main challenges it faces in the investigation and prosecution of crimes committed through the use of information and communications technologies as follows:

(a) Training of actors across the criminal justice system;

(b) The need to equip the judiciary and law enforcement personnel with suitable computing and investigative forensic tools;

(c) Lack of statutory definitions or the establishment as criminal offences of criminal behaviours;

(d) Procedural rules taking into account the special characteristics of digital evidence;

(e) Improving international cooperation mechanisms;

(f) Improving the cooperation of private sector companies (Internet service providers).

7. Argentina also stated that training in the field of cybercrime and in the collection of digital evidence was the biggest challenge in ensuring effective criminal prosecution. Efforts should be focused on broadening the knowledge of the operators of the system and, thus, achieving a better application of the laws and international instruments in force. This would ensure not only an effective response against these crimes, but also respect for the fundamental rights of the parties to the proceedings.

8. Argentina values the contribution of international and regional organizations such as the United Nations (through UNODC), the Organization of American States, the European Union and the Council of Europe, in sharing best practices and experiences. The Ministry of Justice is currently working on the development of model procedural rules for obtaining digital evidence that are to serve as a basis for both federal and provincial legislation.

9. Argentina is a federal country, which, in turn, implies that a federal justice system co-exists with 24 provincial justice systems. This makes it difficult to respond to complex and international phenomena such as cybercrime and digital evidence. A very useful practice that has been implemented is the creation of specialized fiscal units. Ongoing efforts are geared towards ensuring that the different jurisdictions within the country adopt this model and speed up investigations and the exchange of information.

10. Argentina also shed light on the additional challenge of the lack of financial resources to face the transformations that are needed within the judiciary and the security forces, and which encompass sustainable efforts at the State policy level.

Armenia

11. Armenia stated that the relevant State bodies and governmental agencies steadily undertook measures to counter evolving risks stemming from the criminal use of information and communications technologies and, in that regard, to improve sectoral legislation, including through ongoing dialogue with specialized entities of the United Nations, the Organization for Security and Cooperation in Europe, the European Union and the Council of Europe, as well as through enhanced cooperation and information exchange within the framework of the Commonwealth of Independent States Anti-Terrorism Centre, the Collective Security Treaty Organization and the International Criminal Police Organization (INTERPOL).

12. Armenia reported that, for the period of 2019–2020, it envisaged establishing an interagency working group to develop concepts, national strategies and action plans in the spheres of both information and cybersecurity. The working group will be composed of government officials and experts, scientific and research institutions, foundations, and civil society and private sector organizations, as appropriate.

13. Armenia also reported that the draft laws on amending, respectively, the Criminal Code and the Criminal Procedure Code had been drafted, and it was expected that they would be adopted in the near future. That package of bills provides for amendments and supplements to the articles regarding crimes committed with the use of computer systems. During the process of drafting the draft Criminal Procedure Code, a series of meetings had been held with representatives of the police experts of the Council of Europe.

14. Armenia conducts periodic assessments of national money-laundering and terrorism financing risks. In 2017, the most recent assessment for the period of 2014–2017 was conducted. The analytical update of the 2014 Report on National

Assessment of Money-Laundering and Terrorism Financing Risks[1] revealed certain money-laundering risks associated with the use of information and communications technologies. It was found that new products and money-delivery mechanisms (such as online point-of-sale terminals, e-banking, mobile banking and digital wallets) were increasingly used to establish business relationships or carry out complex and unusually large transactions.

15. Armenia noted that products and services involving the use of point-of-sale terminals and e-banking systems had weaknesses in terms of identifying risks that might arise during business relationships. In particular, once a business relationship is established with a customer and the required initial customer due diligence measures are taken, the subsequent business activity of the customer occurs in an online environment, which does not involve face-to-face contact with the relevant bank staff (front office). Such relationships involve fewer opportunities for the identification of suspicious activity. Moreover, data stolen from cards issued by foreign banks can be used to register digital wallet accounts, the activation of which is done through entering a set of valid card identifiers (number, expiry date, card verification value (CVV)). Hence, perpetrators may be able to access financial services without going through mandatory customer due diligence procedures. The registered digital wallets can subsequently be used to carry out multiple wire transfers aimed at disguising the origin of the proceeds of crime, with the subsequent transfer of available balances on the accounts.

16. Taking into consideration the identified risk drivers and factors, the Financial Monitoring Center of the Central Bank of Armenia has been undertaking relevant measures for their prevention and deterrence, including through giving relevant assignments and instructions to particular financial institutions.

17. During 2018, the Division on Combating High-Tech Crime of the General Department on Combating Organized Crime of the Police initiated 79 criminal cases. Of those, 70 were related to hi-tech crime and 9, initiated on the basis of other articles, were closely related to the use of information and communications technologies.

18. According to the findings of a study conducted by the police, there has been an increase in criminal proceedings based on article 181 (Theft committed by means of computer) and article 254 (Illegal appropriation of computer data) of the Criminal Code of Armenia. The study suggested that both individuals and legal entities become victims of acts covered by article 181, while the victims of crimes covered by article 254 are mostly users of social networks or email services. The disclosure of the offences is mainly linked to the fact that they are committed abroad or that traces of the crimes are hidden on the server systems of several countries. Therefore, in such cases, investigations are complicated as a result of differences in the legislation of different countries. As a result, the information requested generally does not reach the requesting law enforcement body.

19. In accordance with relevant provisions of the Council of Europe Convention on Cybercrime, the national contact point within the police has taken measures to detect and reveal users of non-Russian social networks. Inquiries concerning operations or criminal cases were made through the 24/7 contact point network. As reported by Armenia, the specialized subdivision[2] provides professional assistance and advice on sectoral issues to territorial subdivisions of the police upon request (oral or in

[1] The National Assessment of Money-Laundering and Terrorism Financing Risks addresses threats and vulnerabilities in sectors where significant developments are observed, and with regard to which recommendations are provided by experts as part of the mutual evaluation of the system in Armenia to combat money-laundering and terrorism financing by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe. The executive summary is available at: www.cba.am/Storage/EN/FDK/risk_assesment/NRA_Update_Executive_Summary(Public)_eng.pdf.

[2] The specialized subdivision performs operational search activities in compliance with the relevant law, following the assignments given within the framework of criminal cases, and processes applications received from citizens.

writing). In addition, a training course has been organized involving the chiefs of territorial subdivisions of the police during which the characteristics of computer crimes and the process of collecting evidence were explained in detail.

20. Officials from the specialized police subdivisions have visited relevant international organizations and attended tailored workshops and seminars to study best practices in combating cybercrime.[3] Appropriate organizational arrangements were undertaken in Armenia within the framework of Operation Proxy of the Collective Security Treaty Organization, which was aimed at combating the criminal use of information and communications technologies. The police force has been undertaking activities aimed at raising awareness on issues and problems related to the information and communications technologies.[4]

21. The specialized subdivision of the police has been monitoring the Armenian domain zone and the Armenian segment of popular social networks for crime detection. The monitoring is not limited to the detection of cybercrime (for instance, ransomware), but also includes criminal acts (such as blackmail, extortion and forced suicide) in which the Internet serves only as a means for committing a crime and not as a direct tool.

22. Armenia also stated that, in terms of information security, the incitement of identity-based intolerance, violence, hatred, xenophobia and extremist and terrorist practices, along with glorification of perpetrators of genocide acts through the use of the Internet, especially when encouraged and orchestrated at the State level, were of serious concern, entailing the risk of the radicalization of societies and the emergence of foreign terrorist fighters. At the same time, Armenia highlighted that human rights and fundamental freedoms, including collective rights, should be equally and indiscriminately ensured both online and offline, regardless of frontiers[5] and the legal status of territories.

Australia

23. Australia noted that it considered cybercrime as incorporating crimes directed at computers as well as more traditional crimes facilitated by the use of computers. Australia also stressed the need to focus discussions where technical expertise existed. Cybercrime challenges are complex and evolving. Addressing these challenges requires constant attention and the guidance and advice of technical cybercrime experts. In this context, Australia highly values the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime, established pursuant to General Assembly resolution 65/230. Australia considers that the Expert Group, having the relevant United Nations mandate for exchanges on cybercrime, should continue as the primary forum for cybercrime discussions. More broadly, UNODC holds the relevant United Nations mandate to counter transnational crime and drugs. As cybercrime is a transnational crime, it is appropriate for cybercrime discussions to remain focused in Vienna and under the auspices of UNODC. Australia looks forward to the report of the Expert Group in 2021, including its findings and recommendations on national legislation, best practices, technical assistance and international cooperation.

[3] In particular, during an event organized jointly by the European Union and the Council of Europe, advanced methods of combating cybercrime were introduced within the framework of the Eastern Partnership Facility project 2 (Enhancing judicial reform) and project 3 (Support measures against serious forms of cybercrime). Moreover, the draft Criminal Procedure Code, the prospects of legislative reforms and legal grounds for cooperation with the private sector have been discussed.

[4] The activities included interviews to various media outlets, participation in press conferences, issuing a wide range of public information materials and contributing to television programmes.

[5] As stipulated and implied in article 19 of the International Covenant on Civil and Political Rights.

24. In terms of data located offshore, and like all Member States, Australia reported that its national law enforcement agencies faced challenges in accessing and obtaining data to effectively pursue cybercrime investigations and prosecutions. Data was once commonly stored onshore and available under domestic investigatory powers. Currently, owing to rising global connectivity and reliance on cloud computing, data are distributed over different services, providers, locations and jurisdictions. The data can be difficult to locate and are only obtainable through complex and slow international legal cooperation processes. The increasing use of over-the-top communications services means that traditional warrant powers for access to communications held by carriers and carriage service providers do not capture the breadth of data required for cybercrime investigations.

25. Australia underscored that treaty solutions, such as the Council of Europe Convention on Cybercrime, provided an established basis for permitting law enforcement access to data located in another State when, for example, the consent of the person with the lawful authority to disclose the data was provided or the information was publicly available. Restrictions that go beyond these circumstances, including by requiring the consent of State authorities, pose significant challenges to cybercrime investigation and prosecution.

26. Traditional international legal cooperation mechanisms, such as mutual legal assistance, struggle to keep up with demand, causing delays to cybercrime investigations. Alternative international cooperation frameworks between States' competent authorities, law enforcement authorities and, where appropriate and in line with domestic law, communications service providers, can provide practical and expeditious solutions.

27. Australia reported that it successfully used multilateral treaties such as the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime as a basis for international legal cooperation, in addition to its bilateral and domestic arrangements. New mechanisms, such as those contemplated in the additional protocol under negotiation, on trans-border access to data, to the Council of Europe Convention on Cybercrime, respond to the evolving nature of cybercrime and will substantially improve the capability of law enforcement agencies to access data for cybercrime investigations. By enabling more efficient access to data, an appropriate balance can be struck between law enforcement and data protection objectives.

28. In terms of safeguards and police powers, Australia noted that appropriate oversight mechanisms were necessary to balance the safeguarding of human rights and fundamental freedoms against the legitimate need for law enforcement entities to exercise investigatory powers to combat cybercrime. In Australia, law enforcement powers are subjected to substantial oversight, particularly in the exercise of more intrusive powers, such as access to stored communications content and real-time interception. These safeguards include requirements for the judicial authority to exercise power, parliamentary reporting requirements, the right of defendants to challenge the admissibility of evidence and the right of review, and the oversight of all telecommunications warrants by the Commonwealth Ombudsman. Ensuring that police powers are appropriately balanced with safeguards requires ongoing assessment and sustained review, which can be a challenge in some jurisdictions.

29. On the issue of adaptability of legal and operational frameworks, Australia stressed its commitment to maintaining adaptable domestic legislative frameworks that kept pace with rapid technological and behavioural advancement. Australia acknowledges the challenge of drafting laws that cover substantive cybercrime offences, procedural powers for cybercrime investigations and the admissibility of electronic evidence but that remain applicable to evolving technologies and behaviours. To address this, Australia promotes, both domestically and as part of its capacity-building efforts, technologically neutral legislation in which future cybercrime behaviours and technologies are taken into account.

30. Australia reported that its legislation and regulations were modelled on the Council of Europe Convention on Cybercrime, which was the leading international instrument on cybercrime and provided a strong legal and operational basis for international cooperation against cybercrime. The Convention has 63 parties, and more than half of the parties to it are non-members of the European Union. Australia reported that, in its experience, the Convention was modern, progressive and deliberately technology neutral, allowing it to evolve and maintain relevance as new technologies emerges. It had also provided the basis for domestic legislative approaches in regions across the world, including for countries not currently party to the Convention.

31. Australia was also of the view that, in addition to comprehensive frameworks for the criminalization of cybercrime, sustainable and continuous training for front-line law enforcement officers was required. Training should address technology-facilitated crime and the collection and use of digital evidence. Australia considered it important to provide and maintain updated and sustainable training to Australian law enforcement entities, as well as to international partners, through capacity-building programmes.

32. Cybercrime, by its nature, requires close cooperation with other States. Australia has found it challenging when States with whom it must cooperate on cybercrime matters have limited capacity or do not have comprehensive domestic legal frameworks to address cybercrime. Addressing this challenge requires States to focus on strengthening and building capacity to fight cybercrime, including through specialized cybercrime training. Australia underlined that the provision of assistance for legislative reform was also important for developing countries. Australia provides capacity-building and technical assistance to States to assist in building their technical capacity. Australia also supports the valuable work of the UNODC Global Programme on Cybercrime.

Austria

33. Reporting on the global challenges in fighting cybercrime, Austria stated that cybercrime was an evolving challenge affecting every country that required an efficient and effective approach to:

(a) Maximize the number of countries with adequate, compatible cybercrime-related domestic legislation that also supported international cooperation;

(b) Build the cooperation mechanisms, trust and skills to share data to investigate, prosecute and reduce cybercrime.

This includes, but is not limited to, making sure that no safe havens exist for cybercriminals and increasing the capacities of law enforcement and judiciary authorities for effective investigations, prosecutions and convictions of cybercriminals.

34. To ensure comprehensive cyber-related legislation across the European Union, European Union member States, including Austria, have agreed to a set of instruments that provide common definitions for criminal offences: a directive on attacks against information systems, a directive on combating the sexual abuse and sexual exploitation of children and child pornography, and the Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment.[6] Additionally, on 17 April 2018, the European Commission presented legislative proposals to improve cross-border access to electronic evidence in criminal investigations.

[6] The Framework Decision is no longer in force. As at 29 May 2019, it was replaced by the Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment (*Official Journal of the European Union*, L 123, 10 May 2019), pp. 18–29.

35. Nevertheless, access to e-evidence can only be seen as a first step, because there is a lack of a common data-retention scheme at the European level that would safeguard the availability of electronic evidence. Therefore, the time frame and amount of e-evidence vary dramatically between European Union member States and may even depend on the goodwill of organizations. In this context, the problematic WHOIS situation, with regard to which there is still no working solution, is of relevance. The need for better access to electronic evidence will be addressed in a second protocol to the Council of Europe Convention on Cybercrime.

36. Austria noted that, in 2013, the European Union Agency for Law Enforcement Cooperation (Europol) set up the European Cybercrime Centre (EC3), which had made a significant contribution to European Union member States' efforts to fight cybercrime utilizing an agile crime-fighting model. Austria stated that it was necessary to involve prosecutors in cybercrime cases at the earliest stage possible and considered the establishment of specialized networks, such as the European Judicial Cybercrime Network, beneficial.

37. In relation to options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime, Austria noted that cybercrime was a global problem; every nation needed assistance from other countries to fight it. Austria considered that the Council of Europe Convention on Cybercrime represented a model for national legislations and a valuable framework for international cooperation and also considered that it provided a flexible instrument of choice even for parties that were not members of the Council of Europe. Therefore, Austria did not support calls for the development of a new international instrument on cybercrime.

38. Austria stated that the Expert Group to Conduct a Comprehensive Study on Cybercrime was and should remain the main process at the level of the United Nations on the topic of cybercrime at least until 2021. The Expert Group has yielded results, including with regard to legislative reforms based on existing international standards and, in particular, in terms of capacity-building. An update to the draft comprehensive study on cybercrime that was presented in 2013 should be conducted, which would need the expertise of the Expert Group.

39. Austria suggested that UNODC and Member States deliver those goals and that Member States support UNODC in focusing on specific areas where it could have a real impact against the threat of cybercrime, as follows:

(a) Raising police and law enforcement skills for both general and specialist training;

(b) Developing technical assistance in developing nations;

(c) Conducting an analysis of gaps in international cooperation to identify priority areas;

(d) Supporting public awareness campaigns to strengthen crime prevention and build civil society and business cooperation with law enforcement entities;

(e) Strengthening existing operational mechanisms, such as the 24/7 Network;

(f) Collecting data on cybercrime threats;

(g) Acting as a repository of best practices and case studies in tackling cybercrime.

Belarus

40. Taking into account the modernization of modern drug crime and the use of the darknet and cryptocurrencies for drug trafficking, Belarus believes that one of the priorities of Member States should be to ensure the exchange of information, at the supranational level, on means to commit crimes and methods for the detection of criminal activities on the darknet; the gathering and seizure of electronic evidence;

and the development and use of specific techniques in the investigation of the crimes committed in the virtual space. One of the means to counteract the use of information and communications technologies for criminal purposes can be through training law enforcement officers on how the darknet and cryptoindustries function. Belarus stressed that it was important to develop an international legal mechanism (recommendations) on the procedure for seizing the criminal cryptoassets and for storing them until a decision was made by the court.

41. Belarus noted that the Information Security Concept had been adopted on 18 March 2019. It provided for strategic tasks and priorities in the field of information security and countering cybercrime. The Concept is based on the geopolitical interests of Belarus and on the international agreements on cooperation in the field of ensuring international information security, taking into account the main provisions of General Assembly resolutions, as well as recommendations of the Organization for Security and Cooperation in Europe.

42. Belarus believed that the development and adoption of a universal international instrument within the United Nations framework would facilitate the development of cooperation between the competent bodies of Member States in countering the use of information and communications technologies for criminal purposes.

Bolivia (Plurinational State of)

43. The Plurinational State of Bolivia noted that the advancement of technology had an impact on all aspects of human activity in the country and around the world, as well as an impact on security related to the use of new technologies. Information and communications technologies allowed the evolution and spread of traditional crimes through the use of software, applications and communications networks. The dependence of financial institutions on digital systems has facilitated the commission of crimes such as fraud. Likewise, easy access to cell phones without registration of personal data allowed for anonymity in the commission of crimes.

44. For the police in the Plurinational State of Bolivia, crime prevention and ensuring the security of communications are major priorities. A cybercrime division has been created within the Special Force to Fight Crime, a specialized unit to detect crimes committed through information and communications technologies. The national law enforcement agency has dedicated units to monitor the press and social networks. Social media monitoring seeks to prevent “information bubbles” (limiting information in order to negatively affect public opinion) and to prevent extortion, threats, trafficking in persons, fraud, cyberbullying, discrimination and other crimes that threaten the security of the State.

45. The Plurinational State of Bolivia reported that children, in particular, young people aged from 12 to 18, are subject to risks related to the use of information and communications technologies, as they are exposed to these new technologies from a young age and use them regularly for entertainment, communication and information. However, children do not always gain a pedagogical or educational benefit from such technologies.

46. The Plurinational State of Bolivia provided the following non-exhaustive list of types of misuse of information and communications technologies and of computer crimes:

(a) Harassment, insults, slander and social exclusion through social networks, emails and even the comment spaces in the opinion sections of newspapers. In apparently harmless contexts, as in schools, anonymous campaigns are generated through, for example, Facebook, against certain children; university students are subject to slander, such as accusing them of prostitution; and attempts are made to discredit companies on the basis of false information;

(b) Scams and fraud, for example, “phishing”, through which criminal organizations obtain confidential information that allows them to enter bank accounts

and empty them. Another example is the online recruitment of people for jobs as a cover for networks involved in trafficking in persons and child pornography. In general, fraud is related to access to confidential information, as well as the possibility of altering it;

(c) Spam. Although it does not necessarily constitute a breach of the law, spam is the result of the improper use of databases for commercial purposes that many companies use to extend their marketing campaigns to potential users. It may include prostitution campaigns and other campaigns for illegal activities;

(d) Child sexual abuse material is sold by criminal groups over the Internet, in the form of videos and photos. This is a violation of the Convention on the Rights of the Child and the Penal Code;

(e) Intellectual property. The rights of people and innovative organizations are violated in multiple ways, including through the taking of pictures of protected texts (copyright);

(f) Sales on the Internet, including supposed lottery intermediaries and contests.

47. The Plurinational State of Bolivia stated that, along with computer technology development, criminals found innovative ways to commit fraud and other crimes faster than criminal codes could respond. Faced with a phenomenon on the rise, the need for prevention and protection should be seen as the duty of everyone: State, companies, organizations and citizens. In this sense, technological innovations pose multiple challenges for institutions responsible for addressing them, including:

(a) The lack of public awareness and knowledge of the use of information and communications technologies. Such a lack makes people more vulnerable to different crimes. A related challenge is how to develop adequate policies to increase knowledge of the proper use of these technologies;

(b) The existence of a legal vacuum as a result of ignorance or the inapplicability of existing legislation to new crimes involving information and communications technologies. It is therefore necessary to review and update legislation;

(c) The need to modify traditional investigation strategies and anti-crime responses through the use of new methods in view of the evolution of crimes involving information and communications technologies;

(d) The need to become part of international cooperation agreements on research, assurance and obtaining evidence in the field of cybercrime. Several countries in Latin America are already parties to conventions and have made more progress in developing their technological capabilities in the prevention and investigation of crimes committed through information and communications technologies.

48. The Plurinational State of Bolivia recalled that the incorporation of new technologies into governmental institutions affected the organizational culture by modifying procedures and incorporating new assimilated knowledge. Many of the technologies developed and implemented in security institutions require specific knowledge, which might lead to the opening up of institutions to people or organizations that do not necessarily belong to the security area, such as universities, technical institutes, research centres and software suppliers. Currently, both police forces and citizens have various technological tools to deal with security problems and criminal acts, in some cases in the prevention of crime and in others as an aid to the investigation of criminal cases. Some of these elements are quite widespread, among both citizens and the police, while others are more expensive and access for the general public is difficult.

49. The Plurinational State of Bolivia concluded that technological advances had allowed the generation of new criminal dynamics, forcing institutions to adapt and

incorporate innovative strategies that allowed them to stay one step ahead of criminal actors, defending society and preserving public order by preventing and investigating crimes. Therefore, it is inconceivable that institutions responsible for security would consider facing the criminal phenomenon without the use of technological tools. The institutions responsible for security could not only make use of technological tools internally, but could also use them to involve citizens in the prevention of crime.

Botswana

50. Botswana noted the following challenges in combating crimes, especially those aided by the use of information and communications technologies:

(a) Non-harmonized cybercrime and data protection legislation across various countries and jurisdictions makes the investigation of criminal activities in cyberspace very difficult;

(b) The lack of an international framework for exchanging cybersecurity information among various agencies in different countries proves to be a challenge in protecting networks and investigating criminal activities that span multiple jurisdictions;

(c) The advent of new technological innovations such as artificial intelligence and the Internet of Things have the potential to be applied in areas such as agricultural applications, medical applications and climate data analysis, but such innovations also provide a potential platform from or through which cyberattacks may emanate;

(d) A further handicap or major challenge is capacity-building among the various players, i.e., law enforcement agencies, service providers, policymakers and regulators, to address issues of cybersecurity;

(e) Difficulties in dealing with multinational companies that offer services in the country's market while unlicensed, such as Facebook, WhatsApp, Google, Microsoft and Netflix. The process of obtaining information or evidence pertaining to crimes committed over their networks is difficult;

(f) Botswana and many other countries are not parties to existing conventions on information and communications technologies and cybersecurity (e.g., the African Union Convention on Cyber Security and Personal Data Protection and the Council of Europe Convention on Cybercrime), making it difficult to seek recourse using them. The Council of Europe Convention on Cybercrime provides a legal framework for international cooperation on cybercrime and electronic evidence and countries should be encouraged to become parties to it;

(g) Mutual legal assistance processes are slow and cumbersome, making justice inefficient for Botswana and other countries;

(h) Voluntary disclosure of cybercrime in many jurisdictions remains a hindrance. The process of obtaining information is lengthy and in some instances impossible; part of the reason is that rules for accessing subscribers' information are not harmonized among States. What Botswana may construe or consider as a crime may not be so in another State.

51. Botswana made the following recommendations:

(a) There is a need for cooperation and collaboration among agencies such as UNODC, the International Telecommunication Union and INTERPOL to work together to address the challenges of criminals using information and communications technology networks to commit crimes. The roles of the various agencies need to be clarified in addressing cybersecurity;

(b) An international framework should be developed for United Nations Member States to exchange cybersecurity information;

(c) There is a need to have an international policy and regulation framework to address the proper use of new technologies, including artificial intelligence and the Internet of Things;

(d) Capacity-building programmes for Member States should be developed;

(e) A framework should be developed for multinational corporations to provide information and evidence to Member States and to assist in the investigation of crimes committed within the corporations' networks;

(f) The United Nations should be encouraged to investigate the rationale behind the seemingly reluctant stance taken by countries in terms of ratifying regional conventions on information and communications technologies and cybersecurity;

(g) A standard should be adopted for a simpler mutual legal assistance framework, to be adopted by Member States;

(h) Finally, there is a need for an international treaty to address the issues of crime in the information and communications technology network. Such a treaty should harmonize and provide succinct direction with respect to universal legislation, principles of information-sharing, minimum information security standards and assistance in law enforcement matters (investigation, extradition and prosecution).

Brazil

52. Brazil reported that, since the advent of the Internet, its authorities had been dealing with cybercrimes and that such crimes were increasing in number and sophistication. The migration of different offences to digital platforms has demanded major efforts to update the proper legislative and judicial responses to the new threats. The geographical amplitude of those offences has also challenged the traditional mechanisms through which Brazil provides and receives international legal cooperation. The challenges are tremendous: Internet service providers, which hold the information needed to investigate cybercrime and collect electronic evidence, frequently have physical headquarters in one country, provide services on different continents and store their information on servers anywhere else on the planet. In that scenario, law enforcement agents strive to identify and duly address whoever has jurisdiction over the data and direct access to it. Requests for international cooperation, usually channelled through mutual legal assistance treaties, have been very slow to be processed and are sometimes rendered inapplicable, given the pace of digital disposal.

53. Brazil also reported that, whenever there was an international element to investigations and jurisdiction, the legal development of a case was often slowed by divergences over the meaning of privacy protection, which was reflected in the various national requirements for data disclosure. Another challenge to international legal cooperation is the extreme volatility of digital evidence, since the enormous amount of information circulating globally and storage-related costs make companies retain data for no longer than what is strictly necessary for their businesses.

54. Among the numerous crimes that Brazilian law enforcement agents have prosecuted in digital media, child pornography is one of the most frequent. Brazil engages to the highest degree to tackle it, whether through INTERPOL or directly (2 million reports have been received from the United States, for example). Website invasion and phishing are also recurring crimes. Both allow for bank fraud, which has been countered by a proactive and structured response from the Brazilian financial sector. Bitcoin theft and cryptojacking (such as through the WannaCry virus in 2017) are more recent trends; they also pose difficulties for crime categorization.

55. Brazil is sensitive to the peculiar nature of digital evidence and cybercrime. Article 11 of its Civil Framework for the Internet provides that Brazilian law must be applied in the collection, storage and processing of data when one of the computer terminals is located on Brazilian territory. Foreign companies that have branches in

Brazil or that provide services to Brazilian users and that collect, store, maintain or process data obtained from those users must therefore comply with Brazilian law. This framework allows the authorities to have direct access to electronic evidence and data collected from services provided in the country. Brazilian jurisdiction is based on the concept of service offered or provided in its national territory.

56. Brazil was of the view that, although the Internet is a virtual space without borders, its point of connection with the physical world happens in an existing and delimited territory of a State. A cohesive international distribution of jurisdiction is a step forward in prosecuting cybercrimes. A targeting test (similar to the European Union e-evidence initiative[7]) was incorporated into Brazilian law in 2014. Even before negotiations on a global treaty in this matter, Brazil has anticipated future harmonization of domestic legislations by using the legal mechanism of the targeting test, which disregards the location of the servers and the nationality of the custodian company.

57. Brazil stated that more and better cooperation was needed, either through an advanced form of implementation of current mutual legal assistance treaties or through complementary treaties on cybercrime, which would be instrumental to accelerating the international exchange of – the inherently ephemeral – digital proof. The multitude of platforms, systems and strategies that characterizes cybercrime also calls for increased technical cooperation. Relevant experts, police officers, prosecutors and judges should have more opportunities to learn from experiences and methods that have proved successful by their counterparts abroad.

58. Brazil also stated that the multilateral negotiation of an international instrument under the auspices of the United Nations might be a way to establish common minimum standards for the exchange of information and evidence for tackling cybercrime, building on the international and regional instruments that already exist. Such discussions should be organized with the support of UNODC, in Vienna, where there is already expertise in combating cybercrime and where the Expert Group to Conduct a Comprehensive Study on Cybercrime is already discussing the issue. A first step to building a convention on cybercrime could be the convening of an open-ended group of experts to start drafting a text.

Canada

59. Canada reported that, although its laws had recently been updated to better combat crime in the twenty-first century, challenges continued to confront them. Canada highlighted two ways in which the international community had already been working to address the underlying conditions of those challenges.

60. First, from a process perspective, Canada highlighted the important work of the Expert Group to Conduct a Comprehensive Study on Cybercrime. The Group is tasked to conduct a comprehensive study of the problem of cybercrime and responses to it, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. This work is ongoing and guided by a workplan that will see the Group complete its work in 2021. Canada viewed the work of the Group, which provides a forum for expert input into discussions on the highly technical subject of cybercrime, including its international cooperation and capacity-building dimensions, as essential to future discussions in the United Nations about possible responses to cybercrime.

61. Second, from a substantive viewpoint, Canada fully supports the Council of Europe Convention on Cybercrime as the best international tool to combat cybercrime. The Convention deals effectively with the global nature of the criminal

[7] Council of the European Union framework decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (*Official Journal of the European Un*ion, L 350, 30 December 2008).

misuse of information and communications technologies by providing international cooperation in the fight against cybercrime, through the now 63 parties to it, including a significant and growing number of non-European States. The Convention can adapt to emerging challenges through the issuance of guidance notes to help parties apply existing provisions to new phenomena in cybercrime, supplemented by the 24/7 Network and strong capacity-building programmes. The parties to the Convention are also working to improve international cooperation mechanisms because criminal investigations increasingly require access to information stored in other jurisdictions. Canada supports the Convention and firmly believes it is the best available option, either as a legally binding framework for countries willing and able to accede to it or as a model for developing domestic legislation in those countries that do not accede.

62. In terms of challenges created by new technological advances, Canada recalled that communications were ubiquitous: anywhere, anytime, through any provider or on any device. This affects law enforcement. Investigators often must consider the nature of partnering arrangements, ownership of assets and location of entities in a globalized environment. What appears to be a single service to the end user is almost always made up of multiple services, multiple technologies, multiplicity of ownership and distribution across multiple legal jurisdictions.

63. Further, Canada stated that criminal behaviour associated with information and communications technologies continued to change and adapt. It was becoming increasingly profit-driven, transnational in nature and often organized and specialized. Criminal activity was broken up into smaller acts, often conducted by different criminals, each performing one role within the criminal enterprise. This specialization not only increased sophistication but may also afford increased protection because some component elements may not constitute criminal offences in some jurisdictions. Further, the elements of the crime may be dispersed across multiple jurisdictions. Taking advantage of the distributed networks of cybertechnologies does not merely exploit the weaknesses of domestic justice systems but also turns the territoriality and sovereignty of nations against themselves.

64. Focusing on challenges with applying domestic laws when their applicability is limited territorially, Canada reported that laws were typically limited to a specific territory, giving rise to a major challenge since borders were often irrelevant in an increasingly digital world. Information and communications technologies continue to develop and evolve at a dizzying pace, while cybercrimes (involving the misuse or exploitation of information and communications technologies) proliferate and evolve accordingly. The ephemeral and transitory nature of digital evidence adds complexity. It can be quickly deleted or moved at a key stroke from one jurisdiction to another. Further, complications stem from important privacy and human rights concerns and how to accommodate those in a digital environment. Traditional laws provide some investigative powers that remain useful in the fight against cybercrime, but new or more sophisticated legal tools are also needed to ensure that investigative capacity can keep pace with the criminal exploitation of technology.

65. Canada noted that, from a practical perspective, the challenges associated with obtaining the required information from other States included knowing where data are located, whether they are available and whether they are in a comprehensible form. To some degree, this depends on what type of computer data they are. Some kinds of data may be stored to maintain their long-term availability, whereas other kinds of data, such as traffic data, may be more transient. The reach of telecommunications companies is global, but they are generally bound by national or regional laws: how data are accessed or retained can vary from country to country. Canada is concerned about some data-retention regimes, given the considerable privacy implications and their lack of public support. For Canada, investigation-specific preservation regimes, as brought forward in the Council of Europe Convention on Cybercrime, offer a prudent alternative. Furthermore, negotiations on the second additional protocol to the Convention will enhance international cooperation and access to evidence in the cloud.

66. In relation to challenges with the current international cooperation framework, Canada was of the opinion that securing digital evidence, both domestically and internationally, was the lynchpin for the successful investigation and prosecution of cybercrime and other types of serious crime. Yet the consequences of unilaterally crossing borders to secure digital evidence, no matter how vital such evidence, can stress international relations and undermine the validity of such a search.

67. Canada stated that mutual legal assistance treaties are principally used to obtain such information. Canada also stated, however, that current processes were not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for the high volume of requests arising from so many different crimes leaving digital evidence footprints. For Canada, the mutual assistance mechanisms set out in the Council of Europe Convention on Cybercrime are currently the best means of operationalizing international cooperation across a variety of States parties. Furthermore, negotiations on the second additional protocol to the Convention will further enhance international cooperation and provide treaty-based access to evidence in the cloud.

China

68. Welcoming the adoption by the General Assembly of resolution 73/187, entitled "Countering the use of information and communications technologies for criminal purposes", China noted that the General Assembly had emphasized in several resolutions on crime prevention and criminal justice the strengthening of international cooperation in the fight against cybercrime. China recommended that the General Assembly discuss the topic of cybercrime at each of its sessions, including considering the authorization to establish relevant special intergovernmental mechanisms. At the same time, China expressed support for the continued discussion of cybercrime in the framework of the Commission on Crime Prevention and Criminal Justice. It also supported the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime to discuss in depth the substantive issues of combating cybercrime, in accordance with its workplan for the period 2018–2021, and to submit recommendations and conclusions to the Commission on Crime Prevention and Criminal Justice. China also encouraged different regional or international organizations to actively discuss cybercrime issues and work together on responses.

69. In terms of international legislation, China was of the view that the Organized Crime Convention could not effectively respond to the new requirements for international cooperation for addressing cybercrime. There are already some regional conventions in the field of combating cybercrime, such as the conventions formulated by the Council of Europe, the Shanghai Cooperation Organization, the League of Arab States and the African Union. Owing to the differences in the scope of the member States and content of those conventions, international legislation against cybercrime is fragmented. China therefore stated that the international community urgently needed to establish a global legal framework against cybercrime and work together to cope with the increasingly serious crime situation, especially new challenges brought about by new technologies such as cloud computing, artificial intelligence, the Internet of Things and cryptocurrencies. China supported the view that all States negotiate and establish a global convention against cybercrime open to all countries, under the auspices of the United Nations and drawing on the experience of existing regional conventions.

70. According to China, the global convention should effectively coordinate national laws and practices against cybercrime, respond to new problems brought about by technological development in a timely manner and provide universally accepted solutions for global governance of cybercrime. In terms of scope of application, in addition to crimes against computer systems, the convention should also apply to crimes committed primarily through the use of the Internet and information technology, as well as activities aiding and preparing the commission of such crimes. In law enforcement and investigation, the convention should stipulate

targeted law enforcement and investigation measures, and make arrangements for public-private partnership issues, clarifying the obligations of network service providers and operators to cooperate in preventing cybercrime and assisting in law enforcement and investigation. In terms of international cooperation, the convention should regulate the practice of cross-border taking of electronic evidence, design a more efficient mechanism on the taking of evidence, based on respect for State sovereignty and safeguarding the rights of corporates and individuals, and make provisions for the jurisdictional system that are consistent with the characteristics of cybercrime. In addition, the convention should make provisions on capacity-building, technical assistance and crime prevention mechanisms.

71. In terms of international cooperation, China pointed out that, before the introduction of a global convention, countries are encouraged to carry out pragmatic cooperation against cybercrime on the basis of mutual respect, equality and mutual benefit, in accordance with the Organized Crime Convention, regional conventions and bilateral treaties. China also noted that some countries had adopted domestic legislation to bypass the channels of judicial assistance and law enforcement cooperation and had unilaterally taken electronic data abroad, which, in turn, had negatively affected the basic principles of international law such as sovereignty and the protection of individual and corporate rights. China continues to seek a balance between respecting national sovereignty, protecting corporate and individual rights and facilitating investigations, and to improve the efficiency of the taking of evidence by optimizing procedures of judicial assistance and law enforcement cooperation and innovating cooperation models.

72. With regard to domestic measures, China maintained that States should take corresponding measures at the domestic level to effectively combat cybercrime, especially:

(a) Criminalizing the use of Internet for terrorist purposes, and activities aiding and preparing the commission of cybercrime;

(b) Stipulating the obligations of Internet service providers and operators to cooperate in preventing cybercrime and assisting law enforcement and investigation, and at the same time clarify the boundaries of the above-mentioned obligations and guarantee the legal rights of relevant enterprises and individuals;

(c) Enhancing the necessary ability of law enforcement and judicial organs to investigate cybercrime, especially to better cope with the challenges brought about by new technologies;

(d) Recognizing the evidential effect of electronic data and stipulating a definition and scope of electronic evidence;

(e) Clarifying the rules for taking and admitting electronic evidence and prescribing in domestic legislation such means as seizure and sealing up of original storage media, on-site collection, remote inspection and freezing;

(f) Considering the specificity of electronic evidence when applying traditional rules of evidence;

(g) Strengthening the capacity-building of those tasked with taking electronic evidence, cultivating professional teams with both legal literacy and technical capabilities and formulating technical standards for the taking of electronic evidence.

Colombia

73. Colombia agreed with the need to improve coordination and cooperation among States in the fight against the use of information and communications technologies for criminal purposes, through technical assistance to developing countries to improve their national legislation and strengthen the capacity of their national authorities to prevent, detect, investigate and prosecute such criminal activities. However, Colombia considered it important to differentiate between issues related to

cybercrime and a possible broad regulation on information and communications technologies, which would go beyond the criminal regulation of unlawful acts. Therefore, it is very important to be clear about the concepts of the regulation of the use of information technologies and communications for criminal purposes, and the security of information and telecommunications in the context of international security. Colombia was in favour of a free, open and secure Internet and considered it essential that countries had the tools to allow them to cooperate in the fight against cybercrime, strengthen their national capacities and consolidate mutual trust measures between countries.

74. Colombia stated that there were great challenges in the field of cybercrime, for example: digital identity; cooperation with Internet service providers; matters related to digital evidence, techniques for obtaining it, storage, chain of custody, certification and validity; and data protection, privacy and respect for the rights and freedoms of individuals. In addition, cybercrime is closely related to other crimes that transcend borders. Therefore, Colombia was of the view that a deeper understanding of the crimes, their modi operandi, etc., was required and, for that reason, it was important that experiences and good practices be shared among countries to improve national and international responses to counter such crimes. The digital divide makes some countries more vulnerable and cooperation is not ineffective. International judicial cooperation must be adapted to work more quickly (such as mutual legal assistance, requests for mutual legal assistance and mutual legal assistance treaties). For that purpose, Colombia proposed designing protocols and templates that facilitated countries' understanding and would be valid within the framework of the investigation and judicial processes.

75. However, Colombia also considered that the issues related to cybercrime should continue to be discussed, from a technical and political point of view, by the Commission on Crime Prevention and Criminal Justice, through the Expert Group to Conduct a Comprehensive Study on Cybercrime. This should be the main forum, and new, alternative groups should not be generated that limit the participation of countries. The Expert Group has agreed on a workplan, which is expected to result, in 2021, in a report that will contain options for strengthening current responses and proposing new legal and/or other responses.

76. Finally, Colombia considered that it was not necessary to begin the negotiation of a new agreement on cybercrime from scratch. For Colombia, it is essential to prioritize capacity-building and cooperation on the basis of existing treaties, such as the Organized Crime Convention and the Council of Europe Convention on Cybercrime.

Costa Rica

77. Costa Rica referred to its long history of recognition, respect and protection of human rights. Therefore, the international instruments that the country has signed and ratified do not violate the sovereignty of the State.

78. Costa Rica was of the view that prosecutors and investigators in cybercrime cases must strike a balance, while assisting a victim, between the right to privacy of individuals and public security; those guarantees must be respected when collecting evidence and, for that purpose, an application should be submitted to a judge to issue orders for search, the lifting of bank secrecy or the removal of tax secrecy, among others. All this is required to achieve success in investigations and ensure the admissibility of evidence before the court.

79. Costa Rica, being a State party to the Council of Europe Convention on Cybercrime, has had access to extensive training for legal practitioners, as well as access to the 24/7 Network and exchanges with other officials from other regions, in order to obtain and exchange information relevant to investigating in real time and obtaining digital proof. Additionally, since Costa Rica is a State party to the Council of Europe Convention on Cybercrime, it has been included in the Council of Europe

and European Union project entitled Global Action on Cybercrime Extended (GLACY+), under which it has participated in the following:

(a) Mission of the initial assessment of the GLACY+ Project, held in San José from 21 to 24 May 2018;

(b) Consultative mission on legislation on cybercrime and electronic evidence and consultative mission on national policy and strategy on cybercrime. Preparation and revision of the legislative framework on cybercrime and digital evidence and preparation and revision of the national policy on cybercrime, held in San José from 8 to 11October 2018;

(c) Judicial training of trainers on cybercrime and electronic evidence for judges, prosecutors and lawyers, held in San José from 11 to 15 February 2019;

(d) Advanced course on judicial training in cybercrime and electronic evidence for judges, prosecutors and other judicial officials (from 13 to 16 May 2019), and advisory mission on procedural legislation on cybercrime and electronic evidence (on 16 and 17 May 2019).

80. Additionally, the GLACY+ Project has supported the participation of Costa Rica in the following activities abroad:

(a) International workshop on judicial training strategies on cybercrime and electronic evidence held in Cebu, Philippines, from 12 to 14 December 2017;

(b) Joint international conference of the Council of Europe and Eurojust on judicial cooperation in the field of cybercrime, held in the Hague, the Netherlands, on 7 and 8 March 2018;

(c) Fourth Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018;

(d) Twenty-seventh session of the Commission on Crime Prevention and Criminal Justice and the meeting of the Steering Committee of GLACY+ held in Vienna from 14 to 18 May 2018;

(e) Meeting of the Cybercrime Convention Committee (T-CY), 19th T-CY Plenary, 2nd Protocol Drafting Plenary, Octopus Conference on Cooperation against Cybercrime and Seminar on 24/7 Network, held in Strasbourg, France from 9 to 13 July 2018;

(f) International joint workshop for cybercrime investigation units and central authorities held in Singapore from 27 to 31 August 2018;

(g) Fourth Meeting of the Working Group on Cybercrime for Heads of Units, held in Rio de Janeiro, Brazil, from 4 to 6 September 2018;

(h) Conference on Underground Economy and Cybercrime, held in Strasbourg, France, from 4 to 7 September 2018;

(i) Sixth INTERPOL-Europol Conference on Cybercrime, held in Singapore from 18 to 20 September 2018;

(j) 20th T-CY Plenary, 3rd Protocol Drafting Plenary, Meeting of the GLACY+ Committee, held in Strasbourg, France, from 27 to 30 November 2018;

(k) Conference on Criminal Justice in Cyberspace held in Bucharest from 25 to 27 February 2019;

(l) INTERPOL instructor development course held in Bogotá from 25 February to 1 March 2019;

(m) Fifth meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 27 to 29 March 2019.

81. Currently, the Council of Europe Convention on Cybercrime has been ratified by 63 countries (from both the European continent and other regions), which is why, for Costa Rica, it is an international instrument with a record of implementation.

Czechia

82. Czechia reported that it had ratified the Council of Europe Convention on Cybercrime in 2013. In 2014, the ratification of the Additional Protocol to the Convention followed, with a focus on the criminalization of acts of a racist and xenophobic nature committed through computer systems, extending the scope of the Convention and its substantive, procedural and international cooperation provisions. The Convention and its Additional Protocol are open to all countries, not just the States members of the Council of Europe.

83. Czechia strongly believed that the Council of Europe Convention on Cybercrime was the most efficient and most up-to-date instrument to tackle all the challenges arising from the cybercrime phenomenon all over the world. Czechia therefore welcomed the increasing number of non-members of the Council of Europe acceding to or considering acceding to the Convention in the recent period, thus underlying its cross-regional nature and the inclusiveness and transparency of its accession procedures. Consequently, rather than developing a new instrument, which would be rather counter-productive because of the lengthy process of adopting and ratifying United Nation conventions, the focus should be on the effective implementation of existing legal instruments represented by the Council of Europe Convention on Cybercrime, taking into account also its positive contribution to the harmonization of national legislative standards.

84. Czechia supports and praises the specialized expertise guaranteed by UNODC and its specific outcomes, such as the *Practical Guide for Requesting Electronic Evidence across Borders*. The focus should remain on the expert aspects of the issue, provided for by the deliberations of the Vienna-based Expert Group to Conduct a Comprehensive Study on Cybercrime, which provides unique value at the level of the United Nations.

85. Czechia stated that strengthening the procedural rules with a view to combating cybercrime offences was of paramount importance; human rights and rule of law safeguards, including personal data protection, were equally important.

86. Aware of the growing number of threats connected with cybercrime and its increasingly cross-border nature, Czechia reported that it focused on cyberthreat awareness and training, including capacity-building and recruiting new law enforcement staff with the necessary expertise. In that context, the National Network of Public Prosecutors, which operates at the regional level and is specialized in the area of cybercrime, and the establishment of specialized cybercrime police units, were perceived very positively in terms of tackling cybercrime. In addition to this, it was reported that emphasis was given to electronic evidence, the volume of which had been significantly increasing in criminal proceedings. With effect as of 1 February 2019, Czechia adopted a new legal regulation laying down explicit rules for the expedited preservation of stored computer data in national as well as transnational cases.

87. The digitalization of justice was among the priorities of the Ministry of Justice of Czechia. The Government adopted the National Conceptual Strategy on Tackling Cybercrime (the issue is reflected in the regularly updated National Conceptual Strategy on Tackling Organized Crime issued by the Ministry of the Interior), and setting defined targets and measures to be adopted in this field.

88. As regards mutual legal assistance, Czechia reported that requests for assistance and related operations were increasingly processed electronically. The relevant procedures have been streamlined in order to achieve greater efficiency and swift cooperation, including in the exchange of information between States, (for example,

through the establishment of informal channels of communication or points of contact within the 24/7 Network under the Council of Europe Convention on Cybercrime).

89. Czechia mentioned the same potential challenges as other countries: the increasing anonymity of users (encryption as a standard), the availability of malware and paid illegal services (crime as a service) and possibilities to hide profits of crime in virtual currencies, as well as the anonymity thereof. Last but not least, Czechia emphasized that the above-mentioned system of international mutual legal assistance was not sufficient for cybermatters, in particular owing to its slow pace. The average time for handling a mutual legal assistance request involving cyber issues was 21 months (among the States members of the Council of Europe). It is therefore appropriate to start discussing the definition of jurisdiction in cyberspace and direct access to electronic evidence located on servers abroad (or in an unknown place). There is room for a debate on direct cooperation with foreign providers of services. Czechia, as a State member of the European Union and of the Council of Europe, has been participating in numerous discussions in this respect, in particular concerning the European production and preservation orders and the second additional protocol to the Council of Europe Convention on Cybercrime.

Democratic People's Republic of Korea

90. The Government of the Democratic People's Republic of Korea was of the view that information and communications technologies should not be used in criminal activities in a way that threatens or infringes upon the political, economic and social stability of States. It considered that, in order to prevent the use of information and communications technologies for criminal purposes, cooperation and coordination among States were of the utmost importance.

91. Bearing in mind that, worldwide, the legal instruments to prevent and combat the use of information and communications technologies for criminal purposes were insufficient, the Democratic People's Republic of Korea was of the view that it would be necessary to prepare a United Nations resolution regarding cooperation in preventing the use of information and communications technologies for criminal purposes, in accordance with the interests of States.

92. The Government of the Democratic People's Republic of Korea stressed that the issue of the use of information and communications technologies in criminal activities should be discussed in the relevant open-ended expert group meeting involving all concerned States.

El Salvador

93. The Government of El Salvador considered that the absence of legislation was the main challenge in countering the use of information and communications technologies for criminal purposes and, in that respect, it pointed out the following considerations:

(a) The absence of controls or legislation regulating the allocation of mobile telephones and Internet use, for all people in general, in particular, pre-paid telephones, which can be easily acquired and used for any purpose;

(b) The absence of legislation to allow for the obtaining of information online and in real time on usage logs and assignment of public and private IP addresses of the different operators that are in the country;

(c) The absence of a regulation for the use of technological devices, such as drones, signal blockers, interceptors, virus-infected equipment and other equipment that allows acts of cybercrime to be committed;

(d) The lack of regulation obliging network administrators of public, private or non-profit institutions to establish, maintain and safeguard the connection logs of

their internal clients. The lack of such regulation can be exploited for the commission of traditional crime and cybercrime.

Estonia

94. Estonia stated that cybercrime and the use of information and communications technologies for criminal purposes were growing phenomena and created challenges for law enforcement entities worldwide.

95. Estonia noted that, as most of cybercrime offences were of a cross-border nature, international cooperation was of the utmost importance. It is often the case that electronic evidence related to an offence is stored outside the country conducting the criminal investigation. However, international cooperation is not always effective and countries often do not have the necessary substantive and procedural law in place or sufficient capacity among law enforcement entities and the judiciary.

96. Estonia stated that, currently, the only legally binding instrument to fight cybercrime that had a global impact was the Council of Europe Convention on Cybercrime. The provisions of that Convention on both substantive and procedural law and international cooperation have been used as an example by many countries in the world who have not acceded to the Convention. As those standards have been accepted by many countries and a certain level of harmonization already exists, there is a need and possibility for further cooperation. The Convention, as an international legally binding instrument that already exists, provides standards that should therefore be pursued also by those countries that do not have the necessary legal framework in place.

97. According to Estonia, the Council of Europe Convention on Cybercrime had been an effective tool for the gathering and exchange of electronic evidence. As the procedural law provisions and measures of the Convention can also be used for other criminal offences involving computer data or electronic evidence, it is more than just an instrument on cybercrime. In addition, as the provisions of the Convention can be used to address electronic evidence related to any criminal offence, it has become even more useful and valuable for States. Electronic evidence and access to electronic evidence have become one of the biggest challenges for law enforcement authorities while conducting criminal investigations. As electronic evidence is often stored in other countries, international cooperation measures and channels need to be used. Although international cooperation based on the Council of Europe Convention on Cybercrime and other instruments, such as the Organized Crime Convention, works, there is a need to improve it and make it more effective.

98. Estonia noted that, for several years there had been discussions on a second additional protocol to the Council of Europe Convention on Cybercrime. Negotiations had recently started on it. The additional protocol, which would be open to the States parties to the Convention, would provide additional tools for law enforcement authorities and the judiciary in order to improve international cooperation and provide more clear rules and safeguards. Therefore, Estonia stated that the Convention and its global importance and coverage would grow in the future and more countries could take advantage of that.

99. Estonia highlighted the discussions on the fight against cybercrime and capacity-building at the UNODC level. Since 2011, the Expert Group to Conduct a Comprehensive Study on Cybercrime has been discussing possible responses to cybercrime, including how to ensure the better implementation of existing international instruments. The Expert Group has become a useful and effective platform for States to discuss cybercrime-related problems and challenges and exchange best practices. Although there has been no consensus so far on many issues, there has been strong support for capacity-building. The Expert Group is currently continuing its work according to the agreed workplan and is expected to provide conclusions and recommendations by 2021.

100. Estonia was of the view that it would be premature to start parallel discussions and prepare parallel reports at the United Nations level. As resources are limited, they should be used in a most efficient way; therefore, the existing Expert Group should continue and finalize its work within its mandate and workplan. However, as current discussions have already shown, new subtopics and themes related to cybercrime, online investigations and electronic evidence have emerged and that could lead to the continuation of the Expert Group after 2021.

France

101. France reported that, within the context of the Paris Call for Trust and Security in Cyberspace, it had affirmed, together with more than 60 other States and several hundred international organizations, representatives of civil society and the private sector, its support for an open, secure, stable, accessible and peaceful cyberspace in which international law, including human rights, was applicable. Among the conditions to achieve this goal is the fight against the use of digital means for criminal purposes.

102. In this area, France reported that it had a robust national system in the area of combating cybercrime, in terms of existing law, and prevention measures and dedicated resources for investigators and judges to effectively combat the phenomenon. The mechanism stems in part from the transposition of the provisions of the Council of Europe Convention on Cybercrime, which provides an appropriate and flexible international legal framework for tackling the phenomenon of cybercrime by strengthening national legislative systems, but also by paving the way for international cooperation. These provisions are in addition to those provided for in relation to all forms of transnational organized crime under the Organized Crime Convention.

103. Despite this adopted international legal framework and a robust national system, France reported that it still faced certain difficulties in the fight against cybercrime. These difficulties are addressed in the framework of the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime and are as follows:

(a) Lack of adaptation of national laws and specialized means in a number of countries for the fight against cybercrime, in particular a lack of national legislation (both substantive and procedural law) in some countries adapted to the issue of cybercrime and a lack of training and adapted resources for investigators and the actors of the penal chain to effectively combat cybercrime. In order to help strengthen mechanisms in this area, France is actively involved in several capacity-building programmes on a bilateral basis but also at the levels of the European Union and the Council of Europe;

(b) Lack of cooperation on the part of the private sector and some foreign jurisdictions related to data transfer, and even in the conservation of freezing orders in investigations and court proceedings. The cooperation of service providers is still partial at this stage (60 per cent on average, but very variable depending on the partners). It is essential that the latter respond to the requests sent by the competent authorities of the States in the context of investigations and criminal proceedings, without making this response conditional on the nationality attached to the IP address. In order to improve this access to electronic evidence, France is actively participating in the negotiations within the European Union of two legislative proposals presented by the European Commission on 27 April 2018, namely, a draft regulation setting the terms and conditions for access to electronic evidence and a draft directive requiring service providers to designate a legal representative authorized to receive and respond to injunctions. France is also participating in the working group tasked with drafting an additional protocol to the Council of Europe Convention on Cybercrime that also addresses this issue;

(c) The constant challenge of adapting to new technologies, in particular, cryptocurrencies, which are only partially regulated, leading to major risks of the

anonymization of financial flows, the darknet, encryption and the Internet of Things. Discussions on and exchanges of good practices to better understand these phenomena take place within the framework of the Expert Group to Conduct a Comprehensive Study on Cybercrime and more broadly within UNODC, and France wished to underline the operational value of such discussions and exchanges.

Georgia

104. Georgia reported that, since 2008, it had made essential reforms to its substantive and procedural legislation and policy instruments to effectively fight against cybercrime. All major reforms have been aligned with the Council of Europe Convention on Cybercrime, to which Georgia acceded in 2012.

105. Georgia considered the difficulties in transborder data access as a major challenge in the fight against cybercrime. Traditional mutual legal assistance mechanisms have become largely obsolete in the face of constantly evolving cloud computing. Georgia was of the view that deregulating or otherwise easing cross-border data access would be an inevitable reform to increase the effectiveness of the investigation and prosecution of cybercrime. However, these reforms must be carried out by the States through multilateral instruments, and cross-jurisdictional procedural powers must be accompanied by strong safeguards. Georgia considered the drafting of the second additional protocol to the Council of Europe Convention on Cybercrime as an important opportunity in that regard.

106. Georgia reported that, in recent years, it had participated in various capacity-building projects implemented and/or supported by the Council of Europe (Eastern Partnership projects), the European Union and the Government of the United States. As part of those projects, several hundred law enforcement and judiciary professionals have been trained and the Government has adopted various policy documents informed by multinational expertise in cybercrime, electronic evidence and cybersecurity.

107. In terms of substantive law, Georgia reported the criminalization of illegal access and interception, data and system interference as well as the misuse of devices under articles 284–286 of the Criminal Code 1999, in line with articles 2–6 of the Council of Europe Convention on Cybercrime. All cyber-related offences have been prosecuted as conventional crimes with no significant challenges. For instance, cyberfraud is an offence that has been increasing recently, and the Georgian courts have seen no difficulty in applying traditional fraud legislation to such cases.

108. In relation to procedural law, Georgia reported that, since 2010, it had implemented in its legislation all procedural powers provided for in the Council of Europe Convention on Cybercrime, including: production orders, real-time collection of traffic data and interception of content, while several other powers had already existed in its legislation. In the meantime, Georgia has adopted strong procedural safeguards, including judicial authorization for all privacy intrusive procedural powers, the requirement of proportionality, the limitation of the use of certain procedural powers (only used in serious crimes cases) and the requirement to use the least intrusive option of available procedural powers.

109. With regard to cooperation from foreign Internet service providers, it was stated that Georgian law enforcement agencies had been successfully seeking subscriber information from various global Internet companies (Facebook, Apple, Microsoft, etc.), in connection with services offered in Georgia. For example, Georgia was among the world's top 10 countries in terms of disclosure rate, with a 94 per cent disclosure rate from Facebook for legal process requests during the period 2017–2018. In 2018, Georgia introduced an international production order, which empowers a Georgian judge to issue a production order in respect of persons or entities outside of the territorial jurisdiction of Georgia if the following conditions are met, cumulatively: agreement of the person who is the subject of the order with the voluntary disclosure of electronic data; and permission from the host country of

the foreign entity for such disclosure through its laws or executive policies. Such orders must be obtained from a court by the prosecutor and must be transmitted through an official who is authorized by the attorney general. Non-compliance with such orders does not ensue any legal liability. In accordance with article 18 of the Council of Europe Convention on Cybercrime, Georgia has used international production orders in respect of Facebook and other international service providers in connection with services offered in Georgia.

Germany

110. Germany referred to technological development leading to continuous changes in society. It creates new opportunities from which each individual, but also society as a whole, can benefit. On the other hand, technological progress results in new challenges. The technological possibilities for communicating and acting quickly and globally are also used for illegal purposes. Therefore, Germany was of the view that it was important to face up to the challenges and fight criminal behaviour. This requires a sufficiently developed national legal framework, but also functioning cooperation across national borders.

111. For Germany, any solution at the international level should be tailor-made to the specific challenges created by information and communications technologies and should address questions of confidentiality, integrity and access to information systems (so-called core cybercrime). It would be neither feasible nor desirable to try to have provisions that would apply to all crimes committed by the use of a computer or over the Internet. Provisions on core cybercrime need to be flexible enough to keep up with the technological developments. On the other hand, cross-border data exchange mechanisms are needed to investigate, prosecute and punish cybercrime.

112. Germany stressed that the Council of Europe Convention on Cybercrime was well suited to effectively addressing existing challenges in the fight against cybercrime. In this connection, the Convention has proved to be an appropriate tool to combat cybercrime, which is also open to third countries. Germany noted that the Convention was widely accepted by many States as the leading international instrument in the fight against cybercrime and had also been used by authorities in Germany as guidance for domestic legislation. The Convention's technology-neutral definition of offences remains up-to-date. In the view of Germany, it was exactly that focus on, in general, offences against the confidentiality, integrity and accessibility of information systems that contributed to the Convention's high level of global acceptance. Therefore, Germany considered it important to maintain an understanding of the notion of referring to a core set of cybercrime offences. By contrast, caution should be used when extending the scope of "cybercrime" to forms of conduct in which computer devices are only used as a means for committing general offences. Almost any crime can be committed using computer devices, but that does not make them "cybercrime".

113. Germany pointed out that adaptations to more recent developments should be based on the Council of Europe Convention on Cybercrime, as it was currently the case with the negotiation of the second additional protocol, in the field of securing electronic evidence. The second additional protocol would be aimed at improving cooperation between the parties in the field of cybercrime tracing and in the field of securing electronic evidence. Therefore, Germany does not support calls for development of a new international instrument on cybercrime.

114. In addition, the Expert Group to Conduct a Comprehensive Study on Cybercrime is engaged in a comprehensive study on the challenges of combating cybercrime. Substantive discussions on the challenges of cybercrime have been held since 2011 within that Expert Group. According to Germany, the Expert Group is and should remain the main process at the level of the United Nations on the topic of cybercrime. Parallel processes related to General Assembly resolutions and potential duplication of efforts should be avoided, where possible.

115. Germany underlined that special attention should be paid to the implementation of cybercrime legislation and to making effective progress on the ground, including through the provision of technical assistance. There is no lack of adequate international standards, and substantive criminal law legislation on cybercrime has also been put in place by Member States to implement existing standards. The challenge that should now be addressed by the Expert Group to Conduct a Comprehensive Study on Cybercrime is how to provide law enforcement entities with a sound legal framework and the necessary resources to secure electronic evidence and, at the same time, to delimit law enforcement powers through conditions and safeguards based on the rule of law and the protection of fundamental rights and freedoms.

Ghana

116. Ghana reported that it currently had two main pieces of legislation on cyber- and electronic evidence: the Electronic Communications Act 2008 (Act 775) and the Electronic Transactions Act 2008 (Act 772).

117. In Ghana, although the attorney general is the primary prosecutor of all criminal offences, other agencies such as the police also prosecute offences under the authority of the attorney general. The office of the attorney general, however, prosecutes cases forwarded to it by the police. Fewer cases on cybercrime or computer-enabled crimes are forwarded by the police to this office and therefore a few problems and setbacks in the prosecution of such cases have been observed.

118. Ghana reported that the police, the primary investigative body, lacked the necessary tools because the anti-cybercrime forensic laboratory tools had all expired. Investigations are therefore outsourced to private forensic laboratories, with the accompanying cost, which is often passed on to the complainant. Failure to pay for the cost of examination most often negatively affects the trial. Where it is eventually paid, it takes a long time for the police to raise the amount involved. Delay in payment tends to affect the timely release of the report, hence delaying the trial. The cybercrime laboratory is the only one that serves the whole country. However, it lacks the necessary competent staff. That lack of competent staff also gravely affects its output.

119. Ghana reported that there were currently two divergent High Court decisions in Ghana on accessing the contents of an electronic device. According to one of the decisions, a law enforcement agency does not need a court warrant to access the contents of a suspected device; in the other decision, emphasis is placed on obtaining a warrant before accessing the contents. To bring harmony and clarity to the two opposing decisions, a referral has been made to the Supreme Court of Ghana for its determination.

120. Cybercrime by its nature can occur across several international borders. Because of this, critical information needed to prosecute a case successfully may be available in another jurisdiction. Ghana stressed that obtaining access to such information may often be impossible or painfully slow. In the absence of a mutual legal assistance treaty between parties, obtaining the information may not be possible. Where a mutual legal assistance treaty exists, the process of relaying information is often slow and bureaucratic, which causes delays in investigations and the subsequent trial of a case.

Hungary

121. Hungary reported that the number of victims from the misuse of information and communications technologies had increased both nationally and internationally. In general, criminals prefer to utilize Internet-based applications (e.g., Viber, Snapchat, Messenger, WhatsApp and iMessage), compared over technology based on the Global System for Mobile Communications and no special expertise is needed.

This is viewed by Hungary as a challenge for the police and other law enforcement agencies.

122. Hungary also noted that modern information and communications technologies were used as means to commit crimes such as online fraud, the dissemination of online child pornography and online trafficking in synthetic drugs. Social media is also used to easily approach children and commit sexual exploitation, in the form of pictures or videos. In addition, the darknet is exploited to purchase, illegally and anonymously, weapons, drugs and forged documents. Bitcoin is used for payment for those illegal and hazardous products. Moreover, the technology of 3D printing may have potential as an emerging threat when considering the production of weapons or parts.

123. Hungary further underscored that most information and communications technology-related crimes had international features and more than two countries were often involved. This causes difficulties for authorities when a letter rogatory is required for the exchange of information between those States. Authorities may face difficulties when investigating related crimes, for example, because the use of virtual private network services makes it harder to identify the valid personal data of the users. Hence, more efforts are needed in the field of prevention.

124. According to Hungary, national Internet service providers will have to cooperate closely with the public sector, including the police. As there are no international standards on the obligations of Internet service providers, national authorities should harmonize the obligations of such providers on communications-related recording, storage and sharing of information (data retention), including the type of data, the minimum and maximum period of time for preserving data and details of communication. The minimum requirement for sending a request from police to Internet service providers should also be standardized, as providers usually expect more information to process a request than the authorities possess.

125. Hungary would recommend considering as a good practice the 24/7 contact points designated by each member State in the framework of the Council of Europe Convention on Cybercrime. It also proposed utilizing the INTERPOL communications channel for exchanging information.

126. Hungary reported that encryption of personal technical means was useful in the prevention of cybercrime However, encryption is misused by criminals in order to hide their identity and whereabouts. Unblocking encryption is another challenge for the police. Raising awareness about cybersecurity in both the public and private sectors would be required. Furthermore, the upgrading of the information technology infrastructure of institutions and training of public and private sector staff are necessary to improve capacity at the national level.

127. Hungary highlighted that good cooperation between different States was indispensable for cases to be successfully solved. In Europe, Europol had a dominant role in the field of cooperation. The Council of Europe Convention on Cybercrime can be used as a good practice in terms of obtaining electronic evidence from other countries' service providers.

128. As cybercrime is an evolving challenge affecting every country, Hungary considered the following as necessary requirements for efficiently countering it:

(a) Maximize the number of countries with adequate, compatible cybercrime-related domestic legislation that supports international cooperation;

(b) Build cooperation mechanisms, trust and skills to share data to investigate, prosecute and reduce cybercrime;

(c) Make sure that no safe havens exist for criminals and increase the capacities of law enforcement and judicial authorities, particularly in securing electronic evidence.

129. In terms of technical assistance, Hungary recalled the draft comprehensive study on cybercrime in noting that there was a broad consensus that efforts to build capacity

to address cybercrime were essential. The UNODC Global Programme on Cybercrime is in place and the engagement of all Member States is important. There are also a number of other capacity-building programmes that Hungary supports, such as those run by the Council of Europe and the European Union. For Hungary, there is a need to ensure that all capacity-building projects are effectively targeted and coordinated to avoid duplication, appropriately designed and sequenced to meet the needs of international cooperation and to ensure sustainable results, and efficiently evaluated to measure their impact.

130. With regard to options for strengthening existing national and international responses to cybercrime and proposing new ones, Hungary was of the view that the Council of Europe Convention on Cybercrime represented a valid model for national legislation and a valuable framework for international cooperation. Being open to accession by countries that are not States members of the Council of Europe, the Convention provides a flexible instrument for doing so (developing national measures and promoting international cooperation). Hungary does not support calls for the development of a new international instrument on cybercrime.

131. In the view of Hungary, the Expert Group to Conduct a Comprehensive Study on Cybercrime is and should remain the main process at the United Nations level on cybercrime, at least until 2021. It has yielded results, including with regard to legislative reforms, based on existing international standards, and in terms of capacity-building. The past six years have shown good progress in terms of legislative reforms, in particular where countries have made use of existing international standards. Many organizations have set up capacity-building programmes. These efforts need to continue and be further expanded.

132. Hungary would suggest that Member States support UNODC in pursuing the following actions against the threat of cybercrime:

(a) Raising police and law enforcement skills through both general and specialist training;

(b) Providing technical assistance in developing countries;

(c) Analysing gaps in international cooperation to identify priority areas;

(d) Supporting public awareness campaigns to strengthen crime prevention and build civil society and business cooperation with law enforcement entities;

(e) Strengthening existing operational mechanisms such as the 24/7 Network;

(f) Collecting data on cybercrime threats;

(g) Acting as a repository of best practices and case studies in tackling cybercrime.

India

133. India referred to the steady increase in cybercrime, which has raised new issues and challenges for law enforcement. Cybercrime differs significantly from traditional crimes in terms of its nature, scope, means, evidence and activities; therefore, information exchange in real time or near-real time is essential for evidence collection to bring cybercriminals to justice. Cybercrime-related offences are technically complex and legally intricate. Cyberspace and cybercrime have no physical boundaries and, therefore, international cooperation is key for investigation, data and evidence collection and punishment, among others.

134. India reported that, according to its National Crime Records Bureau, 9,622 cybercrime-related offences were recorded in 2014, 11,592 in 2015 and 12,317 in 2016. During 2016, 48.6 per cent of cybercrime cases reported were for illegal gain (5,987 out of 12,317 cases), followed by revenge (8.6 per cent, or 1,056 cases) and insult to the modesty of women (5.6 per cent, or 686 cases).

135. India further referred to the national legal and institutional framework for cybercrime by indicating that the Information Technology Act 2000, as amended in 2008, and the Indian Penal Code provided the legal framework to deal with e-commerce, cybersecurity, cybercrime and cyberterrorism. The national laws are quite extensive and cover most cybercrime-related issues.

136. India also noted that various types of misuse of information and communications technologies in the form of "core" cybercrime and information and communications technologies-assisted cybercrime posed varying challenges which needed to be addressed. The misuse of information and communications technologies covers website intrusions and defacements, viruses or malicious code, denial of service attacks and distributed denial of service attacks, hacking, phishing, cyberterrorism, child pornography, "sextortion", identity theft, cyberstalking and harassment, fake news and propaganda, illegal gambling, sale of fake medicines and drugs, cyberespionage, etc.

137. India pointed out that cybercrime is committed using modern information and communications technology tools such as malicious software ("malware"), botnets, onion routing and even ordinary mobile telephones used for social engineering purposes.

138. With regard to challenges in countering the use of information and communications technologies for criminal purposes, India referred to the following:

(a) The use of many forms of malware and botnets allows criminals to avoid technical controls such as antivirus software and Internet filters, as well as to avoid detection by law enforcement entities;

(b) The use of such technologies with obfuscation, anonymity, computational power and denial of tracing back to the source or perpetrator of crime;

(c) The fact that virtual private network services allow for anonymous communication over the Internet;

(d) The multiplicity of tools that allow criminals to remain anonymous online or untraceable. Of these tools, botnets pose the greatest challenge for a number of reasons;

(e) The fact that addressing cybercrime requires specialized legal knowledge, investigative skill sets, forensic tools and analytical acumen;

(f) In terms of legal challenges, the fact that the transnational nature of cybercrime leads to jurisdictional complexity, thus making investigation and prosecution difficult. The lack of harmonization in legislation among countries leads to difficulties in investigating and prosecuting cyberterrorism offences.

139. Focusing on challenges at the international level that hinder cooperation to combat the criminal misuse of information and communications technologies, India referred to the following:

(a) Time is of the essence in cybercrime investigations and, hence, a time frame for furnishing digital evidence needs to be defined for multilateral cooperation among States;

(b) Mutual legal assistance treaties focus primarily on post-crime scenarios, whereas, unlike traditional crimes, swift information exchange is essential for preventing cybercrime. There is also a need for international cooperation in the field of cybercrime prevention;

(c) Mutual legal assistance treaties have no clause for meeting the needs of emergency requirements, which is a key requirement for tackling cybercrimes. This aspect needs to be discussed;

(d) International cooperation in cybercrime security is essential considering the widespread use of control and command, Botnets and deep web technologies;

(e) Privacy laws hinder information-sharing.

Iran (Islamic Republic of)

140. In terms of challenges in countering the use of information and communications technologies for criminal purposes, the Islamic Republic of Iran reported, as a first problem, the non-compliance of foreign Internet and social networking service providers. Internet and social media have enormously contributed to the improvement of human life. However, the ubiquity and transferability of seamless telecommunication over the Internet and social media have led offenders, especially organized criminal groups, to increasingly utilize such technologies for criminal purposes. Internet and social network service providers have an indispensable role in preventing and countering the use of information and communications technologies for criminal purposes, specifically in the area of electronic evidence collection and preservation, as well as law enforcement.

141. For the Islamic Republic of Iran, a fair and resilient response is significantly dependent on regulating activities in social media. Activities in social media owned by the Iranian private sector are well regulated by the national authorities, in line with the Procedural Law of Computer Crimes. Law enforcement authorities can detect criminal activities in cyberspace, collect and preserve electronic evidence and effectively investigate and prosecute the use of information and communications technologies for criminal purposes. However, given the extraterritorial nature of cybercrime, authorities face serious challenges in prosecuting crimes committed using servers located in other countries owned by foreign public or private sectors. In most cases, foreign social networking services do not cooperate in criminal matters. The non-compliance of such entities with States' requests for cooperation poses a challenge to effective prevention and combating of crimes and puts the rule of law in jeopardy at the national and international levels.

142. With regard to unilateral coercive measures, the Islamic Republic of Iran, situated in a region suffering from organized crime, reported international impediments for cooperation at the international level in criminal matters, particularly in countering the use of information and communications technologies for criminal purposes. Unilateral coercive measures, which are detrimental to a collective response to such crimes, impair the cooperation of countries with Iranian law enforcement authorities in the investigation and prosecution of crimes, in particular, crimes committed through the use of information and communications technologies, as well as in the transfer of the technological tools necessary for preserving electronic evidence and conducting digital forensic examinations. Unilateral coercive measures, as a flagrant violation of the fundamental principles of international law set forth in the Charter of the United Nations, not only hinder effective cooperation on countering the use of information and communications technologies for criminal purposes but also weaken the rule of law, emboldening criminals to pursue their illicit activities. The removal of international impediments remains vital not only to effectively fight against the use of information and communications technologies for criminal purposes but also to ensure the collective security of States. The Islamic Republic of Iran is committed to fighting against organized crime. It supports international cooperation against cybercrime facilitated by UNODC and emphasizes the need to reinforce technical assistance in this area.

143. In relation to the lack of an inclusive international framework, the Islamic Republic of Iran emphasized the need for an international legal framework on cybercrime. Currently, the lack of a sound and inclusive international framework on cybercrime remains a challenge in countering the use of information and communications technologies for criminal purposes. The nature of cybercrime necessitates a context-specific, resilient and collective response through an international instrument, considering the need to keep pace with the development of technology and new modi operandi of organized criminal groups. Existing instruments on cybercrime, having been developed by a limited number of States, lack the requisites for such a response, which, in turn, makes them inapplicable at the international level.

144. The Islamic Republic of Iran commended and appreciated the valuable extensive work of UNODC, in particular the Expert Group to Conduct a Comprehensive Study on Cybercrime. It stated that it continued to support the efforts of UNODC in that endeavour and believed that the adoption of a universal convention on cybercrime under the auspices of the United Nations would be in the best interest of States and would mitigate challenges in the fight against the use of information and communications technologies for criminal purposes.

145. In terms of the legal framework on cybercrime, in the Islamic Republic of Iran, traditional crimes facilitated by or enabled through the use of cyberspace were punishable under the Islamic Penal Code. However, the Islamic Consultancy Assembly (Parliament) has developed and approved cyberspecific legislation to prevent and counter the use of information and communications technologies for criminal purposes, specifically cybercrime, in an efficient and resilient manner. The legislation also covers electronic evidence, owing to its indispensable role in prosecuting cybercrime.

146. From the perspective of substantive criminal laws, the Islamic Republic of Iran referred to the Electronic Commerce Act of 2004. Under that Act, electronic contracts and devices' protective measures for trade secrets were recognized, and the misuse of personal data, infringement of consumer rights and disclosure of classified commercial information in electronic transactions, as well as computer fraud and forgery, were criminalized. It was reported that the Computer Crimes Act of 2009 included provisions on criminalization and the liability of legal persons. Under the Act, inter alia, accessing data and computer systems without authorization, broadcasting obscene content, acting against the integrity and confidentiality of data and computer-related theft and fraud were criminalized. Offences are punishable by a fine and imprisonment of up to 15 years. Article 26 establishes as aggravating circumstances the commission of cybercrime in an organized manner, on a large scale or targeting public service computer systems. The Act is currently under scrutiny to adapt to new modi operandi of criminals and provide law enforcement authorities with a resilient legal framework.

147. From the perspective of procedural law, the Islamic Republic of Iran referred to the procedural law of computer crimes, previously part of the Computer Crime Act of 2009, later incorporated into the Criminal Procedural Law with minor modifications. This piece of legislation covers issues such as jurisdiction, specialized branches for investigation, prosecution of cybercrimes and conditions and procedures for search and seizure of electronic evidence, data and computer systems. The Law ensures due process and protection of privacy. Articles 671 and 672 allow court orders on search and seizure of data only when there are strong and reasonable grounds for the order, which ought to be conducted in presence of the legal owner. Any seizure entailing damage to property or leading to disruption of public service is forbidden, as established in article 679.

Iraq

148. Iraq noted that the use of Internet was one of the characteristics of modern civilization and a measure of development, integration into human civilization and interaction with other countries. Consequently, there has been a revolution in methods of scientific and cultural exchange. The Internet has become a huge channel of knowledge, contributing to the linking and cohesion of societies and individuals beyond geographical boundaries, political and social determinants and intellectual doctrines, the convergence of civilizations and the exchange of ideas across nationalities, languages and religions. This leads to considering which values and principles should govern the content of the Internet: this is still an important and controversial topic. While developing countries make a small percentage of Internet users in the world, the content issue is of great importance to them, because of its impact on their societies. Although one of the values of the Internet is equality and freedom, the privacy of the societies of developing countries requires that

Governments take this particularity into account and try to protect them from multiple orientations and cultures.

149. Iraq stressed that that convergence of peoples also had an effect on the globalization of crime and criminal behaviour, including crimes affecting conservative societies in developing countries. Therefore, there was a need to create regulations on the ethics of the Internet which are commensurate with the specificities of each community. Hence, the development of charters would determine the content of the Internet applicable to each country or area according to appropriate ethical standards, and it would not necessarily be available to all.

150. Iraq highlighted that, in the previous decade, the use of online applications had spread exponentially. Therefore, it has become necessary to organize and regulate them. Some recent applications (for entertainment or games) require subscribers to allow access to a series of personal information. Since the level of access to information available on a network determines the level of privacy of users on the same network, Iraq encouraged designers and promoters of applications to set standards requiring them to show proof of the purpose of accessing information or devices. Another approach is to have volunteers evaluating applications on the basis of agreed standards to increase confidence in proper applications and reduce trust in malicious ones.

151. Iraq reported that it was known that news spread rapidly on the Internet to a wide audience that may not be able or care to verify its source. Companies should be encouraged to deal with the news accurately and objectively and not to publish false news or videos that increase hatred among communities. It may also be required, especially at the present time, to reduce the sources of hate videos, audio and written media. It would also be useful to enhance collaboration between news and social media sponsors and voluntary news assessment teams which analyse the news and explore their credibility.

152. In relation to the online risks for children, Iraq noted that the information society offered an instant digital world with the click of a mouse. An unprecedented level of services and information is accessible through computers or mobile devices with Internet access. Barriers such as costs of devices and access to the Internet are diminishing rapidly. These developments provide children and young people with unparalleled opportunities to become “digital citizens” in an online world that has no borders or frontiers. Online risks and vulnerabilities related to the use of the Internet for children and young people include the following:

(a) Exposure to illegal and harmful content, such as pornography, gambling, self-harm sites, scenes of violence, terrorism and other inappropriate content, and to contact with other users. In most cases, operators of websites containing such content do not take effective measures to restrict access by children;

(b) Targeting through spam and advertisements to promote age- and interest-targeted products;

(c) Compulsive and excessive use of the Internet and online gaming;

(d) Intimidation, harassment, threats and extortion;

(e) Exposure to radicalization and racism and other discriminatory speech and images;

(f) Misrepresentation of a person’s age;

(g) Misuse of personal data and disclosure of personal information leading to the risk of physical harm and infringement of their own or others’ rights, through plagiarism and uploading of content (especially media) without permission, including inappropriate photos.

153. Focusing on public security issues, Iraq underscored that large Internet companies offered great services and opportunities for social and economic development. Online platforms are suitable for socioeconomic development only

when users represent their true selves. However, when they use an anonymous or fake name, which is very common in social media, they may misuse these services and conduct criminal activities such as spreading hate speech, terrorism ideologies and threatening and blackmail messages. This is a difficult public security challenge for Governments of developing countries, especially when they lack high-level technologies and try to seek cooperation from Internet companies. These companies can collect the general and personal information of their customers, as part of the management process of their accounts, by which they can monitor their geographical locations, phone numbers and other useful information, and could prevent crimes and save lives. This calls upon stakeholders to take their share of responsibility, in close collaboration, to address these challenges and ensure safer and continuous services to fulfil the Sustainable Development Goals.

154. Iraq also referred to other challenges faced in countering the use of information and communications technologies for criminal purposes, which include: the unavailability of a global convention on cybercrime; the fact that it is difficult to understand digital evidence, or part of it, and that it is easy to destroy it or make it disappear; the fact that cybercrime is beyond geographical boundaries, coupled with the geographical distance between the criminal and the victim; the lack of adequate training and capacity-building of competent authorities to combat cybercrime; the fact that sometimes the experience and expertise in investigation of cybercrime by non-governmental organizations and other governmental entities is not utilized adequately; the unavailability of adequate electronic infrastructure for the fight against cybercrime; and the difficulty to limiting or constraining the way that cybercrime is committed.

155. Iraq concluded that there was an increasing and urgent need for greater cooperation between stakeholders to ensure a safe digital future.

Ireland

156. Ireland referred to the draft comprehensive study on cybercrime, in which it had been noted that there was a broad consensus that efforts to build capacity to address cybercrime were essential. Indeed, there was widespread agreement at the recent fifth meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime that insufficient capacity currently presents perhaps the most significant challenge in effectively dealing with cybercrime.

157. Ireland highlighted that a significant challenge in relation to capacity-building arose as a result of the fact that any crime may involve a cyberelement, particularly with regard to electronic evidence. It is therefore vital that all investigators, prosecutors and judges possess the relevant expertise in this area. The development of specialist practitioners, where appropriate, is also of importance. This challenge is underscored by the fact that the international nature of cybercrime means that lack of sufficient capacity in one State can negatively impact the ability to combat crime not just in that State, but in any State.

158. In order to overcome these challenges, Ireland noted that it was important that capacity-building programmes at the national and international levels were continued and expanded. These capacity-building projects must be effectively targeted and coordinated to avoid duplication and ensure their sustainability. They should also be appropriately designed with regard to the specific requirements of States' differing legal systems and the needs of international cooperation. Finally, such projects should be robustly evaluated in order to inform the development of future projects.

159. Ireland acknowledged the value of the forum provided by the Expert Group to Conduct a Comprehensive Study on Cybercrime for the exchange of knowledge and experience regarding the challenges posed by cybercrime. In particular, Ireland noted that the nature of the Expert Group as an expert forum, rather than a political one, had been key to its success. As such, Ireland believed that the Expert Group should remain the principal United Nations-level process on cybercrime.

160. Ireland further noted that the primary challenges encountered in relation to cybercrime did not relate to the international legal framework in that area. As such, Ireland confirmed that it did not support proposals for the development of a new international instrument on cybercrime. As the first binding international instrument in the fight against cybercrime, the Council of Europe Convention on Cybercrime has proved both flexible to the ever-changing technological environment and global in scope. The global nature of the Convention is evidenced by the participation of 63 States parties from across all five of the United Nations regional groups, and the fact that a significant number of States that are not parties to the Convention have implemented cybercrime laws modelled on the Convention. In this regard, the substantive provisions of the Convention have largely been implemented in Irish law, and Ireland is committed to ratifying the Convention at the earliest opportunity.

161. Ireland expressed its full support to the ongoing efforts to negotiate a second additional protocol to the Council of Europe Convention on Cybercrime on enhanced international cooperation, which will further improve the Convention and help to ensure that it remains the most important international instrument on cybercrime.

Israel

162. Israel underlined that, in the light of the fact that the privately owned platforms of information technology companies could also be used for criminal activity, one of the most prominent challenges that States were facing today was the interaction between the State and private companies. In this regard, there is a need to consider an appropriate, balanced framework to, on the one hand, allow companies to provide reliable services to their customers, while preserving their privacy and freedom of speech and promoting innovation and, on the other hand, find a proper framework for cooperation with law enforcement authorities in cases of criminal activity.

Italy

163. Italy reported that the Italian National Police, through the Postal and Communications Police Service, was in charge of preventing and combating cybercrime. The 24/7 National Centre for Information Technology Crime and Protection of Critical Infrastructure, set up within the Postal and Communications Police Service, is exclusively tasked with preventing and combating information technology crimes (of a common, organized or terrorist nature) committed against critical infrastructure. It successfully fulfils this task by continually monitoring the Internet. The 24/7 National Centre for Information Technology Crime and Protection of Critical Infrastructure provides cyberprotection services on the basis of agreements concluded between the Department of Public Security and the entities managing critical infrastructure (public-private partnership). The Centre also includes the Italian contact point for technical and operational emergencies related to transnational criminal events.

164. With regard to cyberterrorism, Italy reported that the Postal and Communications Police Service was responsible for preventing and combating online incitement to Jihadi terrorism, particularly through the monitoring of the Internet with the support of language and cultural mediators and in collaboration with the Central Directorate of Prevention Police and the General Investigations and Special Operations Division of the Police). Moreover, notwithstanding the competences of the National Police, the Carabinieri Corps and the Guardia di Finanza, which are in charge of investigative activities in the field of terrorism and subversion, the Postal and Communications Police Service continually update the list of websites used for terrorist purposes. Moreover, the Guardia di Finanza, through the Special Technological Frauds Unit, detects, prevents and counters crimes perpetrated with the use of cybertools in matters of tax evasion, customs crimes, frauds related to European Union resources, currency crimes and counterfeiting.

165. At the European level, the Postal and Communications Police Service acts as the national contact point for the Europol Internet Referral Unit responsible for receiving Member States' reports of online Jihadi terrorist propaganda content.

166. As far as the banking sector is concerned, on the basis of a directive of the Minister of the Interior, the Postal Communications Police Service has been accorded the task of preventing and combating cybercrime where particular techniques of phishing, hacking, or software or hardware technologies are employed in order to fraudulently steal, reproduce and use digital identities, codes for using online banking services and payment cards in electronic transactions.

167. With regard to cryptocurrencies, Italy pointed out that they were often used as payment means to purchase goods and services. These transactions are characterized by the anonymity of both the authors and the real beneficiaries, which encourages their use for illicit purposes (e.g., in the framework of phishing and cryptoviruses of the ransomware type).

168. Italy stated that a national centre for combating online child pornography had been set up within the Postal and Communications Police Service. It continually updated a blacklist to be transmitted to Internet service providers so that they can prevent Internet users in Italy from accessing virtual spaces containing online child sexual abuse materials from other countries. The centre also relies on the cooperation of all institutional and social actors involved in minors' education and protection for the purpose of pursuing common strategies against these phenomena and developing research and new techniques to support investigations. The innovative investigative methodologies adopted by the Postal and Communications Police Service are based on the most sophisticated undercover techniques in order to thwart the anonymization systems and allow for the identification of the subjects involved and of the minors abused. Investigations are also oriented to social networks, which show new forms of enticement and episodes of cyberbullying, as well as online defamation offences (mostly against persons with institutional responsibilities), stalking, harassment, threats and incitement to hatred.

Japan

169. Japan focused, firstly, on a distinct challenge emanating from the nature of cybercrime. Cybercrime offences are highly anonymous and leave little trace. Moreover, cybercrime does not have any territorial or temporal constraints and could cause damages instantly to countless victims. Therefore, criminals are able to execute cybercrime easily by exploiting vulnerable countries which do not have effective countermeasures and use such countries as a basis to operate cybercrime activities against victims throughout the world. Therefore, a common challenge for the international community is to bridge this capability gap so that each country has adequate and appropriate cybercrime countermeasures in place so as not to allow criminals room to manoeuvre.

170. For Japan, the above challenge is further exacerbated by two aspects: lack of legal frameworks and lack of capacity-building. The lack of robust legal frameworks on both substantial and procedural law to tackle cybercrime in some Member States is a major challenge. For example, countries without sufficient legislation to criminalize the creation of computer viruses or countries without legislation that enables the preservation of Internet data pose a serious challenge in countering cybercrime. In order to address this challenge, the international community should assist Member States in enacting new legislation that is capable of addressing new and emerging forms of cybercrime and of withstanding the test of time.

171. According to Japan, the most comprehensive and cost-effective way to achieve this objective would be to utilize existing international legal frameworks. Not only will this avoid duplication of work, but it will also enable Member States to enact legislation with standards that are already widely accepted. This will bridge the gap between Member States and also facilitate international cooperation (for example, the

dual criminality principle will be better met between Member States with similar legal frameworks). In this regard, the Council of Europe Convention on Cybercrime has been widely accepted by the international society and provides for a common starting point. Enacting laws in line with that Convention has proved to be effective in Japan. For example, the offence of "creation of electromagnetic records of unauthorized commands" (article 168–2 of the Penal Code), enacted in 2011 in line with the Convention, has been successfully applied to new and emerging forms of cybercrime, such as the creation of ransomware software, which were not contemplated at the time of enactment.

172. Japan underlined that, even if robust legal frameworks were in place, the lack of capacity in law enforcement agencies and the judiciary to make use of them would seriously hinder any efforts to counter cybercrime. The ability of law enforcement entities to detect, investigate and collect electronic evidence is indispensable in this regard. The judiciary must also understand the modi operandi of cybercrime and properly understand electronic evidence with a view to properly deciding on the admissibility and credibility of such evidence. Japan was of the understanding that at the level of the international community, the provision of capacity-building and technical assistance to Member States in need was still lacking.

173. Japan reported that it had been providing capacity-building programmes to countries in need through, inter alia, country-specific training programmes, including some operated by the Japan International Cooperation Agency, the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders and the Japan-Association of Southeast Asian Nations (ASEAN) cybercrime dialogue. A common challenge is enabling recipient countries to autonomously and sustainably continue their own capacity-building efforts. In this regard, the Government of Japan has cooperated with the INTERPOL Global Complex for Innovation since 2006 to provide countries with the necessary assistance to encourage their own capacity-building efforts.

174. Japan stressed the need to continue expert discussions and underscored that the most effective way to identify challenges relating to legislation and the lack of capacity to render technical assistance to counter cybercrime was to listen to experts' views and experiences. Experts can provide an up-to-date picture on the issue of cybercrime by taking into consideration its evolving nature as well as the new and emerging challenges. Discussions among experts will provide a better understanding of the full magnitude of the problem with a view to identifying where the international community should focus its efforts.

175. Japan referred to the Expert Group to Conduct a Comprehensive Study on Cybercrime in Vienna, which brought together relevant experts from around the world and provided the ideal place to discuss and identify recent trends, challenges and the way forward. The Expert Group is currently discussing pertinent topics on a yearly basis, based on a multi-year workplan that was adopted by consensus among all Member States. The Group is expected to continue its work and conduct a stocktaking exercise in 2021. This exercise will enable the international community to identify the numerous challenges as well as the steps to be taken. Any discussion on cybercrime must be based on specific and evidence-based inputs from experts. Therefore, the outcome of the Expert Group should be considered as the basis for future discussions. The Government of Japan strongly believes that the discussions on cybercrime should be done in the Expert Group, in Vienna. In other words, any movement that will hinder the efforts of the Expert Group, for example, shifting the discussions on cybercrime away from Vienna to a forum in which few experts participate, will seriously weaken the international community's capacity to countering cybercrime.

Jordan

176. Jordan listed the following as the main challenges related to combating the use of information and communications technologies for illicit or criminal purposes:

(a) The existence of free software and programmes which hide users' identities and make it difficult to track and detect them;

(b) The availability and easiness of obtaining information and the possibility of acquiring knowledge and expertise in the use of criminal tools from a multitude of free and widely available websites;

(c) The darknet, which provides a fertile ground for illicit activities including the hiring of persons to commit murder, drug trafficking, trafficking in persons and child exploitation, which renders the monitoring and surveillance of such websites and users a challenging task, owing to the use of encryption to prevent the detection of the identity of users;

(d) Slow procedures and information-sharing in cybercrime cases that take place in several jurisdictions, especially given that cybercrime requires speedy procedures and handling;

(e) The lack of response and cooperation regarding the exchange of information with law enforcement agencies from some social media platforms;

(f) The need for capacity-building through international training programmes and exchange of experience with developed countries in cybercrime matters.

Lebanon

177. Lebanon reported that 2018 had been a busy year in the fight against the use of information technologies for criminal purposes at the level of the executive branch, the parliamentary authority and the judiciary. In the International Telecommunication Union (ITU) Global Cyber Security Index (2018), Lebanon ranked 124 globally, while its Internet usage index rate was 65 (ITU ICT Development Index (2017)).

178. The Government of Lebanon attached great importance to the issue of cybersecurity. A ministerial statement explicitly referred to the enhancement of procedures and measures to protect Lebanese cyberspace and information infrastructure and the personal data of individuals and institutions, which the Government intended to pursue in conjunction with an e-government project entitled "Digital Government". A new ministry (Ministry of State for Technology Affairs) has been established in the new Government.

179. In addition a decision was made by the Prime Minister at the end of 2018 to form a national team for cybersecurity, with the participation of representatives of ministries and relevant departments. The team was tasked with developing a national strategy for cybersecurity in Lebanon and establishing a national authority to deal with that issue. The national strategy being developed includes five key issues. Following a preparation period, the work on the plan began on 15 November 2018, and was scheduled to end within the following two months.

180. Lebanon also reported that parliamentary committees, including the Information Technology Committee and the Committee on Information and Communications, had held several parliamentary sessions to assess the current situation and make recommendations.

181. At the legislative level, Law No. 81/2018, on electronic transactions and protection of personal data, was issued on 10 October 2018, and became effective on 17 January 2019. It deals with multiple and homogeneous issues, including the protection of personal data and crimes related to information systems and data. The law also revises some of the penal code's provisions relating to cybercrime. In

addition, the law addresses issues relating to electronic evidence, obliging Internet service providers to store their customers' log files for a period of three years.

182. Lebanon also reported that, in connection with the Ministry of Justice, 20 judges had been trained, with the support of the Council of Europe and the European Union within the CyberSouth project, to deal with electronic evidence. At the time of submission of the national response, legislative decrees of the Ministry of Justice were being prepared to implement Act No. 81/2018.

183. Lebanon referred to the following as some of the challenges encountered by the Ministry of Justice, in particular, and the State, in general:

(a) Non-issuance of the necessary decrees required to activate Law No. 81/2019;

(b) The ambiguity or insufficiency of some legal provisions contained in Law No. 81/2018, especially in terms of protection of personal data and the designation of a specialized jurisdiction to expedite urgent matters without providing for the establishment of a body to verify that those who practise electronic commerce provide mandatory data (article 31), or with respect to the protection from promotional advertisements (article 32);

(c) The lack of expertise of all judges dealing with electronic crimes or electronic evidence, as well as the need to develop the capabilities of judges and security services and provide them with the training and equipment necessary to enable them to match the capabilities and technical capacity of criminals;

(d) Non-digitalization of the courts and linking them to all ministries and institutions that deal with them;

(e) The need to adopt national cybersecurity strategies and policies at the national level and to establish national institutions to implement these policies and strategies;

(f) The difficulty of dealing with the procedures of the European Union General Data Protection Regulation, which prevents members of the judicial police from directly accessing IP addresses, which were previously available;

(g) Weaknesses of the standard systems used by service providers, such as the Network Address Translation (NAT) networking system for IP addresses, which is used by the Ministry of Communications;

(h) The ability of criminals to hide their real identity by using special software (VPN, TOR, etc.), the difficulty of knowing their actual locations and the use of encryption techniques by criminals to hide transactions. All these prevent competent security services from decrypting and uncovering the information and data of and used by criminals regarding their actual and planned offences;

(i) Multiple devices connected directly to information technology and the Internet, where almost every device (refrigerator, car, etc.) can connect to the network through the Internet of Things without considering the protection systems required before putting these devices in the market;

(j) The absence of a strategic plan for digital transformation in Lebanon and an executive plan for it;

(k) Non-adoption of information security standards and universally recognized policies in various departments and public institutions;

(l) Failure to disseminate a culture of awareness among members of society about cybersecurity and how to protect personal information and data and about the risks of hacking and theft and how to adopt best practices and to protect such information and data;

(m) The phenomenon of the darknet, which allows criminals to illicitly sell and buy goods and substances and secretly practice criminal activities, especially the drug

trade, the sale of weapons and the exchange of child pornography, malicious programs and personal data of individuals;

(n) The phenomenon of virtual and digital currencies that allow individuals and terrorist groups to buy and sell criminal substances in a confidential manner, without the possibility of tracing the sources of such funds or the entities that have been transferred to them;

(o) The absence of an international cooperation framework (convention, treaty) for the exchange of information between States in relation to digital evidence and the fight against cybercrime;

(p) The need for information exchange and concerted efforts between the different security agencies and public and private sector institutions;

(q) Slow communication with local and international service providers;

(r) Not reporting all cybercrime, especially those that cause some embarrassment, such as crimes related to sexual harassment and extortion;

(s) Using criminals for complex techniques such as “distributed attacks” by launching attacks from multiple servers around the world or using some previously hacked “smart” devices as a platform to launch attacks to other targets.

Liechtenstein

184. Liechtenstein noted that cybercrime was on the rise and that the international community was confronted with a diverse range of challenges, including in the areas of investigation and prosecution of such criminal activity. For Liechtenstein, phishing, “CEO fraud”, the hijacking of mailboxes and the illegal interception of data currently pose the greatest challenges. These challenges call for a firm executive and legislative response at the national level and improved cooperation at the international level. However, Liechtenstein is concerned about tendencies to regulate cyberspace as well as criminalize, investigate and prosecute cybercrime in ways that infringe on human rights and fundamental freedoms, including the right to privacy. Liechtenstein noted that States’ obligations under international law, in particular human rights law, must be observed at all times, including when regulating cyberspace and when criminalizing, investigating and prosecuting cybercrime.

185. Liechtenstein reported that its national legislation on cybercrime was based on the Council of Europe Convention on Cybercrime. During the last major revisions of its criminal code in 2009 and 2011, that Convention served as the main international reference framework for the introduction of new cyber-related provisions. Liechtenstein ratified the Convention in 2016 and it continues to serve as the framework for future legislative modifications.

186. Liechtenstein expressed its support for the strengthening of international law aimed at regulating activities in cyberspace, based on the principles of transparency, inclusiveness and cooperation and fully in accordance with existing human rights standards. The Council of Europe Convention on Cybercrime has been ratified by States from all regions and greatly facilitates cooperation among States by harmonizing laws, creating procedures and defining points of contact. Liechtenstein expressed its support for increased international cooperation on the basis of that Convention and opposed the development of parallel or diverging normative standards in the area of cybercrime, a position that it had expressed alongside other concerns in its vote against General Assembly resolution 73/187.

Malaysia

187. Malaysia noted that cybercrime had become more complicated, owing to the evolution of technologies such as the Internet of Things, cloud computing, artificial intelligence, services such as the onion router and the darknet. These technologies are

a double sword: they bring advantages to States and Governments but also to the perpetrators of certain crimes. As a result, Governments are facing more challenges in countering the use of information and communications technologies for criminal purposes.

188. Malaysia noted that the cyberenvironment gave advantage to the perpetrators of crimes owing to the elements of pseudonymity and anonymity and created challenges for law enforcement agencies to identify and link a crime to a specific individual. The widespread use of encryption, which brings tremendous benefit in ensuring confidentiality and integrity, also poses challenges for law enforcement agencies in terms of gathering evidence on cybercrimes. Criminals also enjoy the benefit of the technology to perform their criminal activities. In addition, there are many applications and tools, including anti-forensic tools, available on the Internet which are easily downloaded and can be abused for criminal purposes.

189. Furthermore, Malaysia pointed out that the advent of cloud computing, for instance, provided criminals the opportunity to store information within cloud-based environments. The very nature of cloud computing creates new challenges for law enforcement agencies in terms of discovering and acquiring digital evidence. The discovery and acquisition of digital evidence from remote, provider-controlled cloud platforms differ considerably from on-site or local discovery. Therefore, acquiring data from cloud-based environments requires different tools, techniques and approaches.

190. According to Malaysia, there is a need to address the challenges faced by the personnel involved in handling digital evidence and those related to maintaining the chain of custody and ensuring comprehensive processes and appropriate infrastructure to improve the level of evidence admissibility in court. Technical competency among those involved in handling digital evidence is essential to avoid compromising and contaminating evidence. For example, law enforcement agencies and prosecutors are facing challenges not only in maintaining existing experts but also in acquiring new resources to handle cybercrime investigations. Besides that, there is a need to upgrade the skills and competencies of judges and prosecutors and to enhance their knowledge on the basics of information and communications technologies and cybersecurity, including the terminology related to computer and network systems. As such, specific training for judges and prosecutors on cybersecurity, cybercrimes and Internet technology is needed.

191. In the view of Malaysia, electronic evidence is very volatile and may be simply modified or deleted. Therefore, time is of the essence in evidence-gathering. Malaysia also reported that the lack of human resources among law enforcement agencies was another challenge encountered by the national authorities. Some law enforcement agencies do not even have a team dedicated to focusing on cybercrime investigations. Electronic evidence is usually located in infrastructure belonging to the private sector, namely telecommunications companies and Internet service providers, whose capabilities in retaining and preserving digital evidence vary.

192. As Malaysia stressed, in cybercrime investigations, law enforcement agencies need to obtain cross-border digital evidence through an official channel, mutual legal assistance, in order for the evidence to be admissible in court. Responses received through such assistance might take a very long time, which could prolong court proceedings. In addition, requests for evidence outside the jurisdiction is still subject to the issue of dual criminality.

193. Malaysia also referred to another issue encountered by the Government in countering the misuse of information and communications technologies by criminals: the challenge of making the law respond adequately to current, high-tech cybercrime techniques. In addition, Malaysia highlighted that its domestic legislation required the makers of documents to verify their sources or authenticate the evidence in court. However, the unwillingness of some witnesses, such as global service providers concerning the authenticity of a document or source of information, to testify in court has resulted in non-prosecution.

Mongolia

194. Mongolia underlined that, in the last decade, the use of Internet had been rapidly increasing owing to improvements in its quality, speed and scope. Subsequently, the number of crimes and violations affiliated with the Internet has been growing on a daily basis. Individuals and business entities are frequently attacked by foreign criminal groups through Internet platforms.

195. Mongolia referred to three core elements in the fight against cybercrime: Internet tracking and digital tracing; analysis; and international cooperation. There is a need to increase capacity to fight against cybercrime and to meet international standards in fighting against such crime.

196. Mongolia stated that special attention must be paid to cybercrime, which involved various cyberattacks, pyramid schemes, phishing, online trafficking, online threats, card scheme, online fraud, child pornography and Internet-based intellectual property crimes.

197. As reported by Mongolia, the structure and organization of cybercrime units of other States were divided into three groups: (a) fighting cybercrime against computers, networks and systems; (b) fighting cybercrime using computer, networks and systems; and (c) tracking, strengthening and researching digital footprints. At the national level, however, the country lacked human resources to fight cybercrime, since there was a reluctance to build capacity and human resources in that area. For instance, the Russian Federation has a school dedicated to network security for the purpose of preparing the workforce of the future to fight cybercrime. Currently, Mongolia does not have a dedicated institution to prepare the future workforce to fight cybercrime. Therefore, in the future, in order to fight such crime with the assistance and cooperation of the countries that are leading the fight against cybercrime, Mongolia stressed the need to train and build the capacity of the future workforce and, in addition, to regularly train and prepare current staff so that they had the sufficient capability to combat cybercrime.

198. Mongolia further stated that IP addresses played a crucial role in the investigation of cybercrime and cyberviolations. However, for financial, technological and software reasons, Internet service providers in Mongolia provide one IP address to many users, thus making it difficult to specify the exact time and date of the conduct. Consequently, it is quite difficult to trace the individual who committed a cybercrime or cyberviolation. In order to get the relevant licence from the Communications Regulatory Commission, Internet service providers are required to have the technological capability to make sure that one IP address is shared between a maximum of 20 people. However, the implementation of that regulation was considered by Mongolia as inadequate and ineffective. Therefore, without resolving the issue concerning the IP address, it is nearly impossible to investigate cybercrime swiftly.

199. Furthermore, Mongolia underscored that there was a need to clarify some of the terms implemented in the Criminal Code. For instance, the terms stipulated in article 26 of the Criminal Code of Mongolia such as “electronic devices”, “protected networks” and “illegal attacks” need more clarification; there is a difficulty in their use in practice as there is no clarification or interpretation of such terms in other laws and acts. The rules and regulations of other States with regard to cybercrime are very comprehensive. The elements of such crime stipulated in the Criminal Code are clear; therefore, there is no room for confusion or misinterpretation of the relevant articles.

200. The citizens of Mongolia mostly use Internet-based social platforms such as Facebook, Twitter, Instagram and Yahoo!, which are all incorporated under laws and regulation of different States. Therefore, it is not possible for national authorities to acquire the documents necessary for cybercrime investigations from entities incorporated abroad. There is a document for police-to-police cooperation between Mongolia and the United States with regard to the request for procurement of documents. Nevertheless, on the basis of United States laws, in order to get the

relevant documents it is necessary to obtain a judicial order with respect to the procurement of the documents, which makes cooperation not feasible.

201. In the view of Mongolia, there is a need to adopt a national programme to fight against cybercrime. By adopting such a programme, it would be possible to carry out policy actions against cybercrime in a staged and sustainable manner. Mongolia could improve the current state of regulations concerning cybercrime and create a dedicated unit to fight against such crime.

202. In the current era, during which information technology is developing rapidly, it is crucial to improve national cybersecurity and to fight against cybercrimes. Mongolia was ranked 84 in the ITU Global Cyber Security Index (2018). As information technology grows, cybercrime becomes more complex, involving new types of crime. It is impossible to eliminate cybercrime committed on the Internet. Nevertheless, through the use of relevant laws and regulations, Mongolia is able to respond to it, by means of both prevention and suppression.

203. Moreover, Mongolia stated that the main reasons for becoming a victim of cybercrime were that the public were not aware of the dangers and that adequate knowledge, news and warning about cybercrime were lacking. Therefore, Mongolia stressed the need to build capacity and spread awareness of the potential dangers of cybercrime on the Internet. It is important to enforce strict adherence to technical requirements, monitor the implementation of relevant regulations, resolve short-term IP address problems and other difficulties and increase the responsibility of Internet service providers in order to prevent, suppress, detect and fight against cybercrime.

204. Mongolia pointed out that it was evident from the present situation that law enforcement agencies should be well prepared to prevent and combat such crimes. Therefore, it is essential to train and educate personnel and to increase the capacity of such agencies in every possible way to combat cybercrime. It is also necessary to establish a laboratory responsible for the detection, strengthening, research and analysis of digital footprints and increase the number of units in the fight against cybercrime.

205. Mongolia believed that there was a need to create an international legal instrument to fight and counter crimes involving information and communications technology.

Morocco

206. Morocco noted that the contemporary world was experiencing a revolution in information and communications technologies, including high-end computers and information-processing programmes developed by huge companies. This process has been affected by globalization and the easy transfer of information, bridging the distances between legal and judicial systems. These elements of globalization have resulted in the globalization of crime as well as the methods of committing it. Despite the advantages, information technology has been accompanied by a series of serious negative consequences owing to its misuse and deviations from its intended purposes, mainly through attacks against the fundamental values and interests of individuals, institutions and States. A number of crimes have emerged, committed through the use of Internet and electronic media, which, in turn, makes it easier to perpetrate them and evade the administration of justice (in terms of both the identification and location of perpetrators).

207. According to investigations carried out by the decentralized judicial police services in this regard, Morocco reported that the challenges responding to cybercrime were generally linked to:

(a) Anonymity: use of proxies and the darknet;

(b) Transnationality: the storage of evidence in servers located outside the national territory;

(c) The frequent use of encryption of data;

(d) The criminal misuse of cryptocurrency;

(e) The constant evolution of the modes of operation used;

(f) Difficulties in accessing data on the movement of users of certain applications or sites hosted abroad;

(g) The planning of ongoing training on combating cybercrime for personnel involved in cybercrime investigations and digital evidence, to keep pace with the exponential advances in technology;

(h) The acquisition of adequate and efficient specialized hardware and software to carry out investigations relating to cybercrime offences;

(i) The fact that users of information and communications technologies should be subject to an awareness-raising programme on the risks of non-compliance with protection measures;

(j) The activation of Commonwealth of Independent States protection structures and responses to cyber-related threats;

(k) Inter-State cooperation and coordination on clarifying legal issues and implementation of laws of relevance, as well as on investigative mechanisms and efficiently conducting investigations involving digital evidence.

208. Morocco recalled that the international community had responded to cybercrime through normative instruments, by adopting relevant conventions, and many conferences had been held. By virtue of its strategic location, Morocco also had to adopt legislation to deal with the phenomenon of informatics and to establish partnerships, especially with the European Union, which had been very useful.

209. The Moroccan legislator enacted criminal legislation appropriate to the specificity of the use of information and communications technologies for criminal purposes, in accordance with the general principles of criminal justice. Such legislation included Law No. 03.07, on the Control of Automated Data Processing Systems, adopted in 2003 as part of the Criminal Code (Sections 3/607 to 11/607). This law is the basic framework for the fight against cybercrime in Morocco and its provisions are derived from international conventions, especially the Council of Europe Convention on Cybercrime and its Additional Protocol through Royal Decree No. 1.14.85, issued on 12 May 2014 by implementing Law No. 136.12 approving the Convention on Cybercrime. It was also inspired by the draft law on guidance for combating information technology crimes.

210. Morocco also approved the Arab Convention on Combating Information Technology Offences, signed in Cairo on 21 December 2010, under Decree No. 46.13.1 of 13 March 2013, by implementing Law No. 12.17, published in Official Gazette No. 6140 on 4 April 2013.

211. Article 3 of Law No. 108.13, on military justice, provides for certain requirements relating to crimes that fall under the jurisdiction of the military court, allowing that court to also adjudicate cybercrimes.

212. Preventive laws aiming to protect personal data or electronic data-exchange, such as Royal Decree No. 1.07.129 of 30 November 2007 by implementing Law No. 53.05 on the electronic exchange of legal data, and Royal Decree No. 1.09.15 of 18 February 2009, No. 09.08, on the protection of personal data, make Morocco a destination for investors in the field of information technology and digital economy.

213. Law No. 96-24 on mail and communications issued by Royal Decree No. 1.97.162 on 1 August 1997, as amended and supplemented, and Decree No. 444-08-2 of 21 May 2009 establish a national council for media technologies and digital economy responsible for coordinating national policies and evaluating their implementation.

214. A draft law on organized informational crime under articles 187, 448/1 and 448/2 also provides many tools for responding to this crime.

215. At the institutional level, a judicial police task force has been established to combat cybercrime. In the Moroccan national security apparatus, two counter-terrorism units have been established to combat crimes relating to information systems, at the level of both investigation and tracking criminals through the Internet. The Ministry of National Defence has created the Directorate of Cyber Crimes to deal with cybercrime, trace its effects and combat it in coordination with various national and international security departments.

216. Despite those efforts, Morocco underscored that there were still many challenges in the fight against this crime. It is difficult for legislation to respond to the rapid development of cybercrime and, for example, the lack of legal framework for crimes committed through social networks. Most of the current legal provisions are related to social media users and do not include any requirements to establish the responsibility of network service providers and to oblige them to delete, block, stop or disable access to illegal electronic content. This is compounded by the fact that most of these providers and managers of these platforms are outside the jurisdiction of the country.

217. Morocco highlighted that international cooperation in the fight against cybercrime also posed a challenge in terms of communication with telecommunications service providers in other jurisdictions, which required the adoption of an international instrument allowing direct cooperation with service providers in other jurisdictions to ensure cross-border data connectivity.

218. On the other hand, Morocco also highlighted that tackling cybercrime posed a greater challenge at the level of strengthening the capacity of law enforcement agencies. The large and continuous development of cybercrime techniques, such as Internet-related crime, cyberattacks, phishing attacks, e-phishing, Internet access, virtual currencies, cloud computing and cryptography, require investigative bodies to change their strategies in the search and investigation of criminal inference and provide an electronic directory acceptable to, and authoritative in the eyes of, the judiciary.

Myanmar

219. Myanmar noted that the fight against cybercrime was vital for protecting national cybersecurity and national information infrastructure. There is an urgent need to develop adequate national legislation, compatible with international standards, to achieve maximum effectiveness in fighting cybercrimes. Law enforcement agencies should be provided with the legal instruments, technical tools and infrastructure and appropriate mandates necessary for conducting effective investigation and successful prosecutions.

220. Furthermore, Myanmar stressed that finding the strategies and solutions to the threat of cybercrime was a major challenge for developing countries. With regard to the territorial differences, the offenders of illegal content websites move their activities to a country that does not criminalize illegal content in order to avoid criminal investigations. Such movements to foreign countries are one of the challenges for law enforcement agencies because a server is located outside the territory of the country. Offenders fully exploit such territorial differences and do not disseminate, distribute, share and store illegal content and offensive images on the local hard drives, but on an external server that they can access over the Internet. Accordingly, international cooperation is crucial to identify offenders and overcome the difficulties that come out of the territorial differences. Both consistency with national existing laws and alignment with international standards should be taken into consideration when adopting national cybersecurity policies and creating appropriate legal frameworks.

221. Myanmar reported the following challenges encountered by the State in drafting cybersecurity policy and subsequent legal instruments:

(a) A comprehensive national policy framework and proper legislation on the fight against cybercrime compatible with international practices and procedures needs to be adopted. The State needs to bring its cybersecurity and anti-cybercrime strategies into line with international standards;

(b) A thorough analysis of current national laws is vital to identify any possible gaps and overlaps between cyber legislation and other statutory laws. It is very time-consuming work to review the relevant laws in detail, and it also needs the application of high professional standards and consideration of concepts based on international practices and exchange of views;

(c) The establishment of a law enforcement agency is needed to ensure compliance of the national security and rule of law with the fundamental rights of citizens. Concurrently, a lawful interception centre has to be set up for conducting communication surveillance by adopting lawful interception standard operating procedures based on international principles and standards on data protection and privacy safeguards;

(d) Cyberincidents and cyberattack response teams (i.e., computer emergency response teams, computer incident response teams, computer security incident response teams) which are well qualified for cybercrisis management and threats and vulnerability assessments should be established. Those teams are supposed to disseminate security information and give security advice regarding cyberincidents, cyberrisks and cyberattacks, the potential risks of such cyberattacks to the public and to support law enforcement agencies through the necessary technical assistance to be able to conduct effective investigations;

(e) The State should support funds for taking technical protection measures for creating a safe and secure Internet and for ensuring Internet safety and network safeguards, including by providing the infrastructure, facilities and equipment necessary for implementing such protection measures and safety activities;

(f) While adapting national cyberlegislative frameworks with the purpose of regulating criminal investigations, it is important to take into account human rights safeguards when using personal data;

(g) Clear and precise standards of data protection and privacy safeguards are needed for private sectors involved in collecting, storing or sharing user data;

(h) Internet users should receive well-defined information about cybersecurity, the nature and types of cybercrime and the complicated and complex situation of cyberattacks. In addition, user-awareness campaigns and training should be supported and digital literacy should be upgraded where globally networked information and communications technologies are localized for national users.

222. In Myanmar, online fraud and online defamation cases occur frequently. Common online cases involve using online information and communication to incite racial and religious riots and to threaten government workers and organizations. Myanmar is mainly confronted with the use of social media in terror acts, for propaganda and for personal attacks. In criminal investigations, authorities do not get specific information or cooperation from Internet service providers.

223. Moreover, Myanmar reported that, in cases where subscriber information needed to be requested from foreign-based social media companies, the companies denied the requests on the grounds that the requests did not fall under standard procedures. Consequently, difficulties in investigations are encountered.

224. Myanmar also referred to many difficulties in investigations owing to the lack of resources for technicians, the lack of knowledge of online users and the weak legal binding effect of laws and procedures. As technology is developing and it is possible

to access mobile banking on mobile telephones, cyber-attacks are now targeted at mobile telephone users.

225. Myanmar was of the view that the existing legal mechanisms were insufficient to combat crimes committed through the use of information and communications technologies. It was reported that cyberlaw and related policies on e-Government, e-commerce and cybersecurity matters were being drafted and the project was being implemented under the leadership of the Ministry of Transport and Telecommunications, with advice from an external consulting firm.

226. Myanmar pointed out that solving the problem could be done through the development and adoption of a United Nations convention, as international cooperation was required.

227. Myanmar agreed that responding to the use of information and communications technologies for criminal purposes required a permanent and open discussion, with the participation of all interested States. A platform for such a discussion could be provided by an open-ended United Nations working group with a mandate to develop any documents concerned and make decisions on the basis of a majority of votes. Myanmar also concurred and appreciated that the Expert Group to Conduct a Comprehensive Study on Cybercrime primarily focused on issues pertaining to countering information crime.

Netherlands

228. The Netherlands noted that it was the shared responsibility of the international policing and justice community to prevent the Internet becoming a safe haven for criminals, and crime must not be allowed to pay off. Effective legal instruments respecting fundamental human rights are essential in the fight against cybercrime. Different instruments can be identified: domestic, regional and international. First, many nations have strengthened their domestic ability to combat cybercrime. However, international disparities in criminal law, expertise and equipment exist, which makes it difficult to address and counter a phenomenon of such a cross-border nature. This can only be addressed by enhanced capacity-building efforts within and between States. With a broad international network of able law enforcement agencies, organized cybercrime can be served a significant blow. A second type of instruments is the regional instrument. They are regional, because they are not accessible to countries outside that region. Examples of such initiatives are the e-evidence initiative of the European Union and the frameworks of the Shanghai Cooperation Organization, intergovernmental African organizations and the League of Arab States. Third, there are international instruments open to countries around the world. Examples of such instruments are the Council of Europe Convention on Cybercrime, with 63 parties (and growing) and around 70 additional States for which the Convention is a model legislation, and the Organized Crime Convention and the Protocols thereto. Being one of the early signatories and ratifying States of the Council of Europe Convention, the Netherlands has experienced the benefits of the Convention in terms of yielding results in criminal investigations, through the adaptation of national law to the extended possibilities of cooperation with other State parties. The Netherlands also underlined the benefits of the framework of the Organized Crime Convention.

229. The Netherlands stated that the most relevant and urgent practical needs for law enforcement in cyberspace were, first, cross-border access to e-evidence and, second, international cooperation in criminal investigations. Bilateral cooperation and mutual legal assistance fall short in cases of cross-border and fast-evolving crimes. The need for access to electronic evidence nowadays exists for all types of crime, given the use of information and communications technologies, especially the many new features such as social media and web-based messaging, which have led to an unparalleled rise in digital data. Improved international cooperation can only be achieved if law enforcement agencies have the capacity and capability to participate, for example, in

a joint investigation. Innovative approaches to cross-border access to e-evidence, such as a production order or an extended network search, are already being developed and discussed. Current negotiations on an additional protocol to the Council of Europe Convention on Cybercrime testify to the shared willingness of many States to adapt the existing framework in order to effectively achieve enhanced criminal justice in cyberspace.

230. The Netherlands stated that a big challenge in countering the use of information and communications technologies for criminal purposes was allowing existing instruments to reach their full potential and not divert already scarce resources and energy into a long-lasting process in pursuit of a new supranational framework. The Council of Europe Convention on Cybercrime is already a tangible result that has shown its additional value on a daily basis. Law enforcement agencies and judicial authorities ranging from the United States to Sri Lanka and Japan to Senegal have access to the different possibilities the Convention offers, bringing specific results in criminal investigations. The additional protocol to the Convention is an already ongoing step in the ever-needed efforts to be up to date and offer state-of-the-art solutions.

231. Over time, great efforts have been put into capacity-building, but a lot of work remained to be done, which was the second big challenge. This can be done on a bilateral basis or in conjunction with the Cybercrime Programme Office of the Council of Europe and UNODC. When it comes to the United Nations, the Expert Group to Conduct a Comprehensive Study on Cybercrime is ideally placed to foster a platform for exchanging views and best practices. The Netherlands reported that serious improvement within the Expert Group in the execution of its 2017 workplan had been made during the previous and current years' in-depth consultations. The Netherlands expected that process to lead to a more current and topical overview in 2021 of the challenges for criminal justice in cyberspace, as well as guiding recommendations for the future.

232. The Netherlands called for the improvement of the Expert Group to Conduct a Comprehensive Study on Cybercrime that had taken place in 2017 to be built upon further and expected the most from the emphasis on technical assistance in order to facilitate the transfer of best practices and capacity-building all over the globe. It called for participation in existing negotiations that had proved their value and yielded results. It would call upon fellow States not to divert resources and energy away from those negotiations by initiating new initiatives.

New Zealand

233. New Zealand noted that the geographical isolation of the country had historically protected it from some threats. But the borderless nature of cybercrime means that distance offers no protection. Particular challenges faced by New Zealand in countering the use of information and communications technologies for criminal purposes include:

(a) An incomplete picture of cybercrime in New Zealand and worldwide;

(b) Difficulty in calculating costs of cybercrime;

(c) Difficulty in detecting, investigating and prosecuting cybercrime;

(d) Issues arising from shared responsibilities between Government, non-governmental organizations, the private sector and individuals.

234. In responding to cybercrime, New Zealand reported that it focused on fit-for-purpose legislation, a joined-up approach, awareness and education and international cooperation. The information provided for the purposes of the present report was extracted from the National Plan to Address Cybercrime (2015), available online.

235. There is no complete picture of cybercrime. Cybercrime can be distinguished from "traditional crimes" by the challenges its global nature presents for law

enforcement agencies. Individuals and groups overseas can operate wherever an Internet connection is present. The perpetrators are overwhelmingly based overseas and are highly organized. Worldwide, many instances of cybercrime go unreported. In some instances, victims will be unaware that they have been affected. Other victims are too embarrassed to report the crime, do not know to whom to report it, or do not believe law enforcement entities can provide a remedy. If victims receive a remedy from a supplier or financial institution, they may not also report a crime. Finally, businesses can be reluctant to disclose losses or breaches for fear of reputational damage.

236. The costs of cybercrime are difficult to calculate and the indirect costs from cybercrime, including the opportunity costs, are difficult to quantify. For many small and medium-sized enterprises, cybercrime may result in "denial of business": nothing may be stolen, but an attack can reduce their ability to trade. Businesses and individuals also face costs to protect against cybercrime and for remediation (if required). Cybercrime can also enable the organization and perpetration of physical crime, for example fraud, extortion, disorder and sexual and other violent assaults. Cybercrime may result in social harms through embarrassment and nuisance and, in more serious cases, physical or emotional harm. While the financial losses from cybercrime can be small in an individual instance, the effects on public trust and confidence may be corrosive over time. Cybercrime produces high returns at a low cost and reasonably low risk to the criminal. Thousands of spam emails may generate small losses for each victim, but a much greater loss for New Zealand as a whole.

237. It is difficult to detect, investigate and prosecute cybercrime. The global element of cybercrime makes it difficult to find the perpetrator and access related evidence. Information exchange and cooperation between different countries can be poor and, even where strong cooperative relationships exist, mutual legal assistance treaty processes can be very slow and cumbersome. Cases may require a disproportionate amount of investigative effort, reducing the availability of resources to deal with other demands. The country where a perpetrator is based may also not have the necessary capacity to conduct an investigation or preserve evidence.

238. Investigations are further complicated by the ability to operate near-anonymously on the Internet. Attribution in cyberincidents is very difficult, particularly when an attack originates overseas. This makes cybercrime challenging not only to investigate but also to prosecute. Proxies and channels such as Tor and peer-to-peer networks can be exploited by criminals attempting to hide their identity under layers of encryption. Those networks are frequently used to facilitate criminal activity and pose challenges for law enforcement agencies. Such networks and darknet sites are also selling cybercrime as a service, such as hackers for hire or simple toolkits. These developments lower the barriers for entry into cybercrime. Accordingly, a group of unskilled actors can have a relatively damaging impact. At the other end of the spectrum, the lines are blurring between criminal actors and State actors (some of whom may also act with criminal intent) as activity proliferates and techniques become increasingly sophisticated. As technology and detection strategies evolve, so too do the actors, making it difficult for responders to keep pace. Offenders are not averse to using anonymizing technology, including the use of software such as Tor, to attempt to hide sites providing child exploitation material and drug dealing.

239. New Zealand's response to cybercrime is shared between the Government, non-governmental organizations, the private sector and individuals. A range of government agencies in New Zealand have policy and operational responsibilities related to cybercrime. Those roles have largely evolved organically rather than by design. Cybercrime is a shared problem and non-governmental organizations, civil society and the private sector all have a role to play in both prevention and response. This shared responsibility can lead to challenges. Some incidents will be reported to multiple places, and victims may be passed between agencies in an effort to find the best place for a resolution. Responses may also vary within each service. New Zealand has made progress in this area with the establishment of CERT NZ in 2016. CERT NZ is a body that provides more clarity about where to report cyberincidents,

more efficient triaging of cyberincidents to relevant agencies and more actionable and timely advice to agencies, businesses and individuals. Many private sector companies also provide a response to cybercrime as a part of their core customer service. There are opportunities for the Government to improve the experience for victims of cybercrime, while also gaining a better understanding of the issue and raising awareness.

Nicaragua

240. Nicaragua was of the view that the current penal provisions were insufficient to combat crimes committed using information and communications technologies. Many countries have been victims of such crimes. Hence, Nicaragua was convinced that the topic should be addressed by the United Nations, with a view to developing and approving an international agreement on cooperation and regulation on the subject.

241. Likewise, Nicaragua considered it opportune to establish, as soon as possible, an open-ended working group with a view to advance the drafting of an international regulatory instrument regarding the crimes committed using information and communications technologies.

Norway

242. Norway referred to its national input sent to UNODC on 4 March 2019 concerning measures and initiatives against cybercrime in relation to the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime.[8]

243. Norway ratified the Council of Europe Convention on Cybercrime in 2005 and was following the process to develop the second additional protocol closely. Norway supports the Expert Group to Conduct a Comprehensive Study on Cybercrime as the main process at the level of the United Nations on the topic of cybercrime, at least until 2021.

244. Norway noted that, as threats in the area of cybercrime were developing, the responses to the challenges must be scaled up, as lack of effective measures may constitute a threat to the rule of law. Electronic evidence is becoming increasingly relevant in criminal cases. These data are often stored abroad, thus making it difficult to locate and obtain. Cooperation is instrumental at both the national and international levels. As law enforcement agencies are limited by national borders, more effective international frameworks are needed. At the same time, adhering to fundamental rights and having a high degree of awareness of safeguards when developing new international instruments must be at the centre of efforts.

245. Norway confirmed it would ensure sufficient capacity, competences and technical ability to meet new and constantly changing types of crime. Norway referred to the need to increase the understanding of the threats faced in the digital sphere as being at the core of its national work. It is also important to see the new challenges in the context of more traditional crime. Cybercrime is not an isolated type of crime: it is a cross-cutting element in many types of crime, including transnational organized crime and terrorism. Concerted action between Governments and the private sector is a central part of the solution.

246. Norway further highlighted that the Norwegian authorities would, according to the International Cyber Strategy for Norway (2017), ensure close coordination between bodies that represented Norway in arenas where international cybersecurity policy and cooperation on cybercrime and handling cyberincidents were developed. In the continued international efforts to combat cybercrime, Norway would support

[8] Available at www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

collaborative approaches to finding good solutions while upholding democratic values and protecting universal human rights.

Peru

247. Peru reported that, in 2016, the Inter-American Development Bank, in coordination with the Organization of American States, had prepared the 2016 report on Cybersecurity in Latin America and the Caribbean. After the evaluation of 49 indicators that addressed different areas (politics and strategy, culture and society, education, legal frameworks, and technologies), four main challenges were identified for Peru as follows:

(a) Strengthening the cyberprotection capabilities of the armed forces;

(b) Strengthening the technical capabilities of the Division for the Investigation of High-Tech Crimes (DIVINDAT) for the handling of electronic evidence;

(c) Strengthening the social awareness of cybersecurity;

(d) Improving the capacities of university teachers and training to companies.

248. According to the *Microsoft Security Intelligence Report* (2017), 16.9 per cent of computers in Peru were infected with malware, compared with the world average of 7.8 per cent. Likewise, infection through Trojans (8.13 per cent), worms (5.7 per cent) and viruses (0.92 per cent) in Peru is above the world average.

249. In a recent study, the Digital Government Secretariat of the Presidency of the Council of Ministers of Peru indicated that 22.6 per cent of public administration entities did not have the capacity to implement their generalized system for digital security. The following reasons were given:

(a) Insufficient economic resources necessary for the implementation;

(b) Insufficient staff (50.9 per cent);

(c) Insufficient knowledge to start the implementation (22.6 per cent);

(d) It is not a priority issue for their sector (16 per cent).

250. The negative impact of information security risks is severe on the critical assets of the organization, generating economic and passive costs for entities. In several cases, main business processes are interrupted or stopped while they are blackmailed or extorted for the payment of large sums of money for the retrieval of information.

251. As for priority challenges, the Government of Peru considered necessary the creation of a specialized prosecutor's office for computer crimes, greater training for tax staff on the matter and an institution to be responsible for preventing cybercrimes among citizens. There has been a significant increase in the number of complaints in computer crimes, especially in the form of computer fraud. The main challenges that must be faced are the following:

(a) Computer fraud through "carding", in which criminal organizations use the confidential information of bank cards to make online purchases from Internet stores with web domains and servers located abroad. This makes it difficult to obtain information in a timely manner by regulating the laws in each country that cover the information that each company must provide;

(b) Identity theft through social networks as a result of the freedom with which users can create an account and navigate anonymously, even creating different names that are used illegally;

(c) Child grooming, in which criminal organizations pretend to be children in order to induce their victims to undress in front of the video cameras of laptops or computers. In other cases, face-to-face meetings are held, during which child sexual

abuse material is obtained to be sold and exchanged with other paedophiles, nationally and internationally, including through applications such as WhatsApp;

(d) Blackmail and extortion by people against their ex-partners involving videos or photographs of a sexual nature that they threaten to publish on the Internet. This may be done for different purposes, such as obtaining an economic benefit or resuming a relationship;

(e) Attacks by activist hackers in execution of campaigns whose objective is to affect the institutional image and make use of anonymous networks, such as Tor, that enable attacks to originate in Asian countries, making their identification impossible. Likewise, attacks on institutional information for commercial purposes are occurring, with the aim of obtaining extensive information from entities, for criminal purposes. There is also the possibility that media outlets undertake cyberattacks or cyberespionage in order to get access to news-worthy material.

Philippines

252. The Philippines referred to cybercrime as a serious social issue and noted that cyberspace was considered as a new dimension (in addition to land, air, and water), which the Government had to regulate and law enforcement agencies had to extend their mandates in order to address. To ensure the safety and security of the people, the Government has recognized the need to equip law enforcement agencies through the following legislation: Cybercrime Prevention Act, 2012 (Republic Act No. 10175), Electronic Commerce Act, 2000 (Republic Act No. 8792), Anti-Photo and Voyeurism Act, 2009 (Republic Act No. 9995), Anti-Child Pornography Act, 2009 (Republic Act No. 9725), Anti-Trafficking in Persons Act, 2003 (Republic Act No. 9208), Access Device Regulations Act, 1998 (Republic Act No. 8484) and Data Privacy Act, 2012 (Republic Act No. 10173).

253. The Philippines acceded to the Council of European Convention on Cybercrime on 20 February 2018 and has accommodated international requests for data preservation, the provision of subscriber information of users, the collection of computer and business data and the seizure of domain names.

254. In this context, the national laws consider specialization as key to a successful investigation and prosecution of cybercriminals. Under the Cybercrime Prevention Act of 2012, the following specialized authorities were created to deal with cybercrime and related issues:

(a) Office of Cybercrime of the Department of Justice: as the central authority under the Cybercrime Prevention Act to ensure the implementation of the Council of Europe Convention on Cybercrime, including matters in relation to international mutual assistance and extradition;

(b) Cybercrime Investigation and Coordinating Centre: an inter-agency body under the administrative supervision of the Department of Information and Communications Technology, by virtue of Republic Act No. 10844 of 2015, responsible for policy coordination among relevant agencies and the formulation and enforcement of the national cybersecurity plan;

(c) Cybercrime Division of the National Bureau of Investigation: this was reorganized to effectively improve its cyberresponse, digital forensic and cybersecurity capability, as set out in the Cybercrime Law. It created three cybercrime regional centres and acquired new and updated forensic tools and software, with corresponding training for its digital examiners;

(d) Anti-Cybercrime Group of the National Police: established along with nine regional anti-cybercrime offices all over the country. It has developed four specialized anti-cybercrime courses, which are required for police officers who specialize in cybercrime.

255. The Armed Forces of the Philippines, spearheaded by the Deputy Chief of Staff of the Communications, Electronics and Information Systems Service, was crafting a Cyberspace Strategic Plan to provide a roadmap for the realization of a fully cyberspace-capable organization by 2022.

256. The Anti-Money-Laundering Council is the country's financial intelligence unit tasked to implement the anti-Money-Laundering Act, as amended by Republic Acts Nos. 9194, 10167, and 10365, as well as Republic Act No. 10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012.

257. In January 2017, the judiciary also contributed to efforts to combat cybercrime by designating cybercrime courts to adjudicate cases covered under Cybercrime Prevention Act of 2012, in addition to being designated as commercial courts.

258. The Philippines also reported that, at the national level, the following inter-agency cooperation mechanisms had been established:

(a) The Sub-Committee on Cybercrime of the National Law Enforcement Coordinating Committee, which strengthens inter-agency coordination to combat cybercrime and other cybercrime-related activities by providing assistance to the anti-cybercrime campaigns of other States, such as by facilitating information-sharing and arrests of persons involved in cybercrime;

(b) The Inter-Agency Council against Trafficking, which promulgates rules and regulations for effective implementation of Republic Act No. 9208, or the Anti-Trafficking in Persons Act of 2003, as amended by Republic Act No. 10364, or the Expanded Anti-Trafficking in Persons Act of 2012. It is headed by the Secretary of Justice, which in turn results in faster programme and project coordination to effectively address issues related to trafficking in persons. It recommends measures to enhance mutual assistance among foreign countries, through bilateral and/or multilateral arrangements, to prevent and suppress international trafficking in persons;

(c) The Inter-Agency Council against Child Pornography, headed by the Secretary of Social Welfare and Development and composed of other relevant government agencies and non-governmental organizations, formulates comprehensive and integrated plans and programmes to prevent and suppress any form of child pornography and in the filing of cases against individuals, agencies, institutions or establishments that violate the provisions of Anti-Child Pornography Act of 2009 (Republic Act No. 9775).

259. In terms of good practices in law enforcement and investigation, the Philippines recognized the importance of utilizing specialized agencies in law enforcement and investigation. For the Philippines, inter-agency cooperation is crucial for an effective enforcement and investigation of cases, with the Sub-Committee on Cybercrime of the National Law Enforcement Coordinating Committee, the Inter-Agency Council against Trafficking and the Inter-Agency Council against Child Pornography as leads.

260. It was also noted that another mechanism being utilized by law enforcement agencies was INTERPOL, with the INTERPOL National Central Bureau in Manila functioning as the main coordinating body for domestic and international police cooperation in addressing transnational crimes. Close cooperation with law enforcement agencies, other government agencies and foreign law enforcement agencies is essential in order to investigate, trace and prosecute perpetrators of cybercrime.

261. The Philippine Centre on Transnational Crime, which is secretariat of the INTERPOL National Central Bureau in Manila, and the Anti-Money-Laundering Council co-hosted the INTERPOL operational meeting on the stolen funds of Bangladesh Bank, one of the biggest money-laundering cases.

262. With regard to good practices in electronic evidence and criminal practice, the Philippines reported that digital forensics were used by specialized agencies to trace, investigate and prosecute cybercrime offenders. The Cybercrime Prevention Act of 2012, approved on 12 September 2012, became effective on 18 February 2014.

Coupled with the use of the rules on electronic evidence issued by the Supreme Court, the prosecution of cybercrime cases in cybercrime courts became more efficient.

263. The Cybercrime Investigation and Coordinating Centre launched the National Cybersecurity Plan 2022 on 2 May 2017, in which the urgency of protecting every single Internet user in the Philippines, the national critical information infrastructure, government networks, small and medium-sized enterprises and other businesses and corporations was recognized.

264. Even with the efforts being made by the Government to combat cybercrime, together with specialized agencies, the enactment of laws to combat cybercrime, the creation of cybercrime courts and the use of rules on electronic evidence, there is still the need to provide training to specialists and experts in the use of these tools. Ongoing capacity-building, especially from sponsorships, whether local or foreign, should be taken advantage of. Additionally, assessments and evaluations of cybercrime and cybersecurity should be made periodically to take stock of where the Philippines is headed in its efforts.

Portugal

265. Portugal stated that information and communications technologies created new opportunities for criminals and led to a rise in the rate and diversity of crimes committed in and through the digital world. Such crimes have an increasing impact on the stability of the critical infrastructure of States and enterprises and on the well-being of individuals, owing to their implications for the full enjoyment of human rights and civil liberties. The use of the technologies and of the Internet for the dissemination of terrorism content, for the promotion of hate speech and for extremism and radicalism, as well as for the commission of other serious crimes such as sexual abuse of children, trafficking in persons and money-laundering are examples of the concerns of States in the digital era.

266. Portugal noted that States were facing difficulties in criminal investigations as a result of the use of encryption technologies, the difficulty of obtaining and preserving electronic evidence, the exercise of jurisdiction in cyberspace and the lack of international cooperation in that field. The use of encryption meets a legitimate need for privacy and the exercise of fundamental rights, as well as the needs of businesses and public authorities; companies have invested in developing tools that offer better protection of their customers' privacy, saying that efforts to weaken encryption may expose private information to people who may misuse it. Secure processing is an important element of the protection of personal data, and encryption is recognized as a security measure in regulation 2016/679 of the European Parliament and the Council of the European Union. However, while keeping data or information secure, encryption technologies offer good opportunities for criminals as well.

267. Another challenge to investigations and prosecutions is how to obtain and secure electronic evidence stored in computer systems, given its magnitude and complexity. Network-based services may be provided from anywhere, without requiring the presence of physical structures, facilities or personnel in the State concerned. Consequently, relevant evidence is often stored on servers outside the investigating State, in one or multiple foreign jurisdictions, or even in an unknown jurisdiction, and may involve multinational service providers.

268. Owing to a lack of connection between investigation authorities in different jurisdictions, requests for judicial cooperation mostly require cross-border access to electronic evidence and are often addressed to States that host a large number of service providers but have no specific relationship with the procedures. Obtaining evidence through judicial cooperation may take lengthy periods of time, during which such evidence may be no longer be available. A further difficulty is that there is no clear framework for cooperation with private service providers, and national approaches to such cooperation vary.

269. Portugal referred to preventing and combating incitement to terrorism and the spread of terrorist content and the promotion of radicalism and extremism over the Internet and through other information and communications technologies as other challenges that States faced at the international level.

270. The fight against crimes committed through information and communications technologies and cybercrime is a matter of strategic concern to Portugal, and it is strongly committed to that fight. A law on computer crime (Law No. 109/1991) was adopted in 1991 and revised in 2009 (Law No. 109/2009 (Cybercrime Law)). The National Strategy on Security in Cyberspace (2015) is currently under revision and a new National Strategy is expected to be published in the coming months. The use of information and communications technologies and cybercrime are mentioned as one of the most important issues in both the old and the new strategies.

271. Portugal also reported that a law on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks had been approved. It was particularly important for the criminal investigation of serious crimes as terrorism and organized crime.

272. Portugal considered that a proper and modern domestic legal framework, providing for proper procedural tools and powers and, thus, allowing law enforcement authorities and prosecutors to investigate and collect digital evidence while respecting the rights and safeguards of both suspects and victims, was crucial for fighting cybercrime.

273. Portugal has developed specialized units in its law enforcement agencies and judiciary: within the Public Prosecution Service, a Cybercrime Office was created in 2011 and, within the Criminal Police, a National Unit for Fighting Cybercrime and Technologic Crime was established, which operates and coordinates at the national level. The Public Prosecution Service is responsible for criminal investigations and the Criminal Police is the law enforcement authority with exclusive competence to investigate cybercrime and crimes committed through the use of information and communications technologies, acting under the direction of the prosecutor in charge, as specified in the Law on the Organization of Criminal Investigation (Law 49/2008). This specialization increases the efficiency of investigations and ensures consistent responses and international coordination. International cooperation for obtaining evidence from another country is important, and efforts should be made, especially at the United Nations level, to build capacities and increase cooperation.

274. In terms of further challenges, Portugal noted that cybercrime and the use of information and communications technologies to commit crimes were not territorially bound; they were committed globally. Global services (such as webmail services, social networks and cloud services) are used everywhere and may also be used for criminal purposes targeting victims from many different States. While some States recognize the need for expeditiousness in cases involving digital evidence, other States insist on the use of traditional tools such as mutual legal assistance requests, which do not allow for responses to the current requirements or challenges in due time. There are no comprehensive international regulations in place and national frameworks provide for diverse solutions; therefore, a new approach is needed.

275. Portugal also mentioned that the parties to the Council of Europe Convention on Cybercrime were drafting an additional protocol to the Convention. Such a protocol is expected to provide clear guidance to law enforcement entities and the judiciary on cross-border access to data and improving informal cooperation, information-sharing and the functioning of mutual legal assistance to obtain data stored in other jurisdictions, while fully respecting fundamental rights and freedoms.

276. At the European Union level, a regulation and a directive on electronic evidence are being negotiated, which will allow for the securing and gathering of e-evidence and for the improvement of cooperation in this field.

Qatar

277. Qatar stated that the misuse of information resources and technologies, including through cybercrime and electronic piracy, was increasing, affecting the security and stability of countries. The adverse effects of the use of information resources or technologies on development, peace, stability and human rights have been reviewed in detail in various resolutions of United Nations entities. Crimes committed in the digital world, and their increasing diversity, and the use of such technologies and means for purposes inconsistent with the objective of maintaining international stability and security adversely affect the integrity of States' infrastructure and damage their security in the field.

278. There is a need to strengthen legal measures at the national and international levels to address cybercrime and to propose new measures to combat, detect, investigate and prosecute cybercrime. It is necessary to intensify international efforts to prevent the use of criminal resources or information technologies for criminal and terrorist purposes. For the maintenance of peace and stability and the creation of an open, secure, stable and peaceful information and communications technology environment, Qatar reaffirmed its support for the Expert Group to Conduct a Comprehensive Study on Cybercrime and called for its continuation.

279. Qatar reported that it sought to enhance the security of information within the State and to encourage international cooperation in the fight against cybercrime, especially as it had been the victim of electronic piracy, which had served as a cover for creating an artificial regional crisis that had seriously damaged regional and international security and stability. Qatar pays special attention to the development of its legislation and the promotion of joint international action to prevent, detect and prosecute the perpetrators of digital crimes.

280. Qatar issued Law No. 14 of 2014 to combat cybercrime, which represented an advanced step to strengthen national legislation and procedures to combat cybercrime. The law included chapters defining cybercrime, such as crimes of infringement of information systems, programmes and networks, electronic fraud and counterfeiting and the crimes of infringement of intellectual property rights. The law includes provisions on procedures for investigation, collection of evidence, obligations of service providers, obligations of State agencies and international cooperation, including mutual legal assistance and extradition.

281. Qatar concluded that cybercrime, as an emerging form of transnational organized crime, was a growing and changing challenge. It requires coordinated and growing collective responses based on the principle of common interest and shared responsibility. In this context, Qatar seeks to strengthen its cooperation with UNODC with a view to building national capacities, enhancing the security of computer networks and promoting regional and international cooperation in order to provide a secure and robust cyberenvironment.

Romania

282. Romania stated that, while technology advanced, it played an important role in a wide range of criminal activities, with a great impact and influence on the online environment. The term "cybercrime" represents a broad range of criminal threats such as the distribution of ransomware and other malware, fraud involving non-cash payments and the online trade in child sexual exploitation material.

283. Romania characterized "cyber-dependent crime" as any crime that can only be committed using computers, computer networks or other forms of information and communications technology. "Cyber-facilitated crimes" can be conducted either online or offline. The role played by the Internet is to increase the scale, geographical scope and speed of these crimes. Online child sexual exploitation represents the worst aspect of cyber-facilitated crimes. Moreover, the darknet hosts a growing number of

forums dedicated specifically to the production, sharing and distribution of child sexual exploitation material. The Internet additionally offers a wide range of applications, such as peer-to-peer file sharing and secure data storage, which facilitate these crimes.

284. Romania made reference to fraud involving non-cash payments as another highly organized, highly specialized and constantly evolving threat, adapting to counter-measures and new technologies. This threat includes two distinct crime types: card-not-present fraud, largely committed online, and card-present fraud, which typically occurs at retail outlets and bank machines. Criminals are also taking over the operating systems of bank machines to access cash more easily.

285. It was reported that online commercial platforms could also be used for trade in illicit goods and services. Illicit online markets, on both the surface web and the darknet, provide tools, such as cybercrime toolkits or fake documents, that may be used to commit other crimes.

286. Compromised data were further mentioned as another commodity commonly traded online and subsequently used for the furtherance of fraud. Typically, these are financial data such as compromised payment card data or bank account login details. They may also include data ranging from lists of full personal details and scanned documents to email lists and online account logins.

287. Romania stated that criminals made use of every communication channel available, not just for internal communications, but also to contact potential victims, for example, through email phishing campaigns or social media. Criminals also use secure applications and similar services to hide their criminal activities. The growing use by criminals of encryption services and other malicious actors poses a serious impediment to the detection, investigation and prosecution of all types of crimes, including terrorism.

288. New forms of payment, such as cryptocurrencies and online payment and banking platforms, have afforded criminals new ways of financing and expanding their criminal businesses. The rapid processing of transactions across multiple jurisdictions and the proliferation of encryption and anonymization tools represent some of the most significant obstacles encountered in financial investigations. Bitcoin is the most commonly used currency for criminal-to-criminal payments relating to cybercrime. It is accepted on most darknet marketplaces and automated card shops, but it is increasingly used for crimes outside cyberspace, such as ransom payments for kidnappings.

289. Romania highlighted that cybercrime in the country had evolved in a similar fashion to other global crime phenomena, as described in reports by Europol over the period 2014–2017. Criminal groups originating in Romania have been remarkably active in cybercrime. Over time, Romania has also become a target of such crimes. They pose a threat to national security in a broad sense, including the financial system.

290. Romania reported that it had undertaken major efforts to adopt comprehensive procedural legislation to cover different aspects of the criminal proceedings for the gathering of electronic evidence, in line with rule of law safeguards and remedies, based on the Council of Europe Convention on Cybercrime. Romania ratified the Convention in 2003. National legislation criminalizing illegal activities, as prescribed in articles 2–9 of that Convention, covers a large range of misconduct, allowing for investigation of relevant cases by specialized units. These provisions are still – 15 years after their enactment – applicable to new forms of cybercrime. Additional guidance on the constituent elements of the crimes is provided by the guidance notes adopted by the Cybercrime Convention Committee.

291. As reported, in 2004 the Directorate for the Investigation of Organized Crime and Terrorism was established within the Prosecution Office of Romania. Moreover, within the police, the Directorate for Combating Organized Crime was established as a specialized structure to support the activities of the Directorate for the Investigation

of Organized Crime and Terrorism. In the last five years, more than 28,800 cases of cyber-dependent or cyber-enabled crime have been investigated.

292. Romania referred to an example of such offences, namely “skimming” activities used to compromise bank cards, involving activities of criminal groups in many different jurisdictions (manufacture of parts, assembly of parts and the actual fraud). These activities fall under article 365 of the Criminal Code. In terms of the modus operandi, social engineering, spear-phishing, multiple levels of command and control servers and vulnerability scanning continue to be some of the most used techniques. A great challenge for law enforcement is the increasing use of open-source tools by a wide range of actors, thus making it difficult to attribute an illegal activity to specific persons or groups. Malware attacks are covered by national legislation in article 207 (blackmail) and articles 362 and 363 of the Criminal Code.

293. Social engineering tactics for committing fraud (phishing, spear-phishing, vishing, smishing), as well as man-in-the-middle or man-in-the browser techniques used mostly for hijacking money transfers, constitute common forms of cybercrime in Romania. They are criminalized under articles 325 and 249 of the Criminal Code (depending on the specific case, additional charges, such as misuse of devices or data interference, can be brought). The use of the Cobalt Strike platform for attacks against the banking system are investigated under the provisions of articles 360, 362–363, 366 and 249 of the Criminal Code.

294. Cryptocurrency mining and most crypto-jacking activities are investigated under articles 360 and 366 of the Criminal Code. Deep insert skimming activities are also investigated under articles 360 and 366 of the Criminal Code.

295. Romania concluded that the creation of a comprehensive legal framework based on the Council of Europe Convention on Cybercrime and of specialized institutions had helped address the ever-changing problem of cybercrime and electronic evidence. At this point, more resources and further training and capacity-building are needed. Discussions on new international treaties in this field would not be useful and may dilute efforts.

Russian Federation

296. The Russian Federation noted that the challenge of countering the use of information and communications technologies for criminal purposes, in terms of dimensions and extent, had long become a global threat affecting all countries of the world without exception. At present, the world community does not have a unified approach to this issue. At the international level, the situation is compounded by the lack of a comprehensive international legal framework for cooperation and even a common terminological basis. At the regional level, relevant instruments have been developed and adopted by a number of organizations, but their capacity to deal effectively with such crimes remains insufficient.

297. The Russian Federation stated that a number of States promoted the Council of Europe Convention on Cybercrime as a possible solution. However, this instrument is inadequate to address current threats. The Convention was developed at the end of the 1990s, and therefore it does not regulate many modern “inventions” of criminals. It also allows for the possibility of violating the principles of State sovereignty and non-interference in the internal affairs of other States. Thus, there is still a threat of legitimizing access by special services of a limited group of countries to the uncontrolled collection of personal data belonging to users all over the world as well as of continuing the trend set by a number of States to consolidate their technological gains in the information space and maintain the “digital gap” between developed and developing countries.

298. The Russian Federation stressed that it promoted the development of universal principles and norms that would be shared by all interested parties and that would lay the foundation for effective international cooperation in countering cybercrime. Such

an instrument could be a convention against crimes in the use of information and communications technologies, under the auspices of the United Nations, which would take into account the current realities and principles of sovereign equality and non-interference in the internal affairs of States. The Russian draft of a United Nations convention on cooperation in combating cybercrime, which was circulated as an official document (A/C.3/72/12), could serve as a basis for such work. The Russian Federation believed that that project would become "food for thought", would initiate a debate on the topic in key international forums, primarily the United Nations, and would consolidate and focus the efforts of the international community on the development of practical solutions in this area.

299. In the view of the Russian Federation, given the global nature of the phenomenon of information crime, it is not enough merely to discuss the issues only within the framework of the Vienna forum of the United Nations – the Expert Group to Conduct a Comprehensive Study on Cybercrime. The mandate of the Expert Group is limited to discussing, for the most part, technical aspects of this issue. In the present context, the search for a political solution and consensus-building are conceived as the primary task.

300. To this end, the Russian Federation emphasized that the provisions of General Assembly resolution 73/187, on countering the use of information and communications technologies for criminal purposes, should be firmly implemented. Another solution is to launch a permanent forum within the General Assembly to discuss, on the basis of an integrated and balanced approach, all the aspects of international cooperation in the fight against cybercrime, which would be aimed at finding a political solution and consensus-building, taking into account the urgent needs of States in this area and facilitating the exchange of best practices in this field. One of the options for such a forum is to establish an open-ended United Nations working group on cybercrime with a mandate to develop and implement any relevant documents by the Member States.

Saudi Arabia

301. Saudi Arabia referred to the following obstacles to combating the use of information and communications technologies for criminal purposes:

(a) Poor cooperation by digital platform companies with legal and law enforcement authorities around the world;

(b) The absence of digital identity in the virtual world and the use of identifiers and phantom data and the impersonation of other persons on the Internet, especially on social media;

(c) Different legislation and criminal laws of Member States;

(d) The lack of coordination, cooperation and assistance among countries in the fight against cybercrime;

(e) Inadequate controls on the provision of electronic services (networks, resources, cloud environments, services, etc.) in many countries;

(f) The lack, in many countries, of advanced information systems that would allow for the monitoring of suspicious operations and identifying their sources and those behind them;

(g) Poor human and technical capabilities of government and private institutions and individuals in cybersecurity;

(h) The lack of international legislation to criminalize and trace the use of information and communications technologies for criminal purposes that could contribute to international efforts to combat them;

(i) The need to develop the qualifications of people in the field of information security through specialized training programmes;

(j) The multiplicity and variation of legislation and laws between countries that penalize criminal behaviour in the field of information technology;

(k) The objective of online commerce platforms is solely to make profit. In addition, such platforms provide a fertile ground for software and applications that use technology to hide users and commit cybercrime;

(l) The extent of crimes committed using information technology and its cross-border potential, resulting in poor coordination and communication among States to confront such crimes;

(m) Replacing traditional currencies with digital currencies makes it easier for criminal groups to hide many of their financial transactions on the Internet;

(n) Poor awareness of the safe and optimal use of information technology and the Internet;

(o) The need for Saudi Arabia to participate in international legislation to combat the misuse of technology;

(p) The need to intensify prevention by raising awareness among communities about methods used by criminal gangs active on the Internet.

Serbia

302. Serbia reported that the organization and jurisdiction of the Special Prosecutor's Office for High-Tech Crime of Serbia were specified in the Law on Organization and Competences of Government Authorities for Combating Cybercrime, which came into force on 25 July 2005, and the Law on Amendments to the Law on Organization and Competences of Government Authorities for Combating Cybercrime, which came into force on 1 January 2010. Accordingly, the Special Prosecutor's Office has jurisdiction over the territory of Serbia to proceed in cases involving the aforementioned crimes.

303. Serbia referred to its legislative and strategic framework, which includes:

(a) Law on Organization and Competences of Government Authorities for Combating Cybercrime;

(b) Law on the Confirmation of the Council of Europe Convention on Cybercrime;

(c) Law on the Confirmation of the Additional Protocol to the Council of Europe Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems;

(d) Law on the ratification of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse;

(e) Criminal Code;

(f) Criminal Procedural Code;

(g) Law on Electronic Communication;

(h) Law on Information Security;

(i) Strategy for the Fight against High-Tech Crime for the period 2019–2023;

(j) Strategy for Information Society Development in Serbia until 2020;

(k) Strategic Assessment of Public Security in the Republic of Serbia.

304. Recent reforms of domestic legislation emphasize the importance of the Council of Europe Convention on Cybercrime and its Additional Protocol.

305. In September 2018, the Government adopted the National Strategy for Combating Cybercrime and the accompanying Action Plan. Furthermore, the Ministry

of Justice established working groups for amending the Criminal Code and the Criminal Procedure Code. For that purpose, representatives of the Public Prosecutor's Office and the Special Prosecution Office for High-Tech Crime initiated an expert mission in March 2019 within the iPROCEEDS joint project of the European Union and the Council of Europe. Their task was to conduct an in-depth legal gap analysis of national legislation, evaluating its compliance with the Council of Europe Convention on Cybercrime, Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/22, and other European Union and international standards. The analysis will result in proposals for amendments of the laws, in order to achieve complete harmonization.

306. Serbia indicated that experience from the past 15 years demonstrated that capacity-building and specialization at the domestic level, based on existing international agreements, worked very well and made a difference. It is questionable whether discussions on new international treaties in this field are helpful.

307. In relation to the institutional framework and administrative capacity, Serbia listed the following institutions which are competent to act in the field of cybercrime:

(a) Special Prosecutor's Office for High-Tech Crime;

(b) Higher Court in Belgrade;

(c) Department for Combating and Suppressing High-Tech Crime of the Ministry of Interior;

(d) Other competent State authorities.

308. In terms of statistics and analysis, Serbia reported that the total number of cases filed in the registry of the Special Prosecutor's Office for High-Tech Crime in 2018 was 3,022, of which 322 cases were filed in the register of known adult perpetrators; 1,306 cases were filed in the register of unknown perpetrators and 1,394 cases filed in the register of other criminal offences, which was an increase of 27.46 per cent compared with 2017.

309. Consequently, as Serbia further reported, significant positive developments were also observed in the application of various procedural actions at various stages of the criminal proceedings, such as filing criminal charges against 324 known perpetrators, an increase of 28.57 per cent; the application of deferred prosecution increased by 85.71 per cent, and the application of a plea agreement increased by 105 per cent. This significant increase is the result of an increase in the number of persons and cases reported, an increase in the human resources of the Special Prosecutor's Office and an increase in capacity-building for competent authorities.

310. Regarding good practices, Serbia mentioned the following examples of international cases in which specialized cybercrime authorities of Serbia participated and which were successful owing to the implementation of the Council of Europe Convention on Cybercrime and international cooperation provisions implemented in Serbian law:

(a) Operation "Shadow Web", in February 2018. The takeover of one of the biggest criminal forums, "In Fraud", dealing with stolen credit card information. One Serbian citizen was arrested and criminal charges were filed;

(b) Operation "Power Off", in April 2018. The takeover of the largest criminal service for distributed denial-of-service attacks in the world, "Webstresser". Two Serbian citizens were arrested and criminal charges were filed. The competent authorities of Austria, Canada, Croatia, Germany, Italy, the Netherlands, Serbia, Spain, the United Kingdom and the United States, as well as Hong Kong, China, participated. The Special Prosecution Office for High-Tech Crime commenced investigations into two suspects and, for the first time, cryptocurrency was seized from one suspect;

(c) Operation "The Dark Overlord", in May 2018. This related to a criminal group that stole personal data and blackmailed their owners.

311. Serbia reported that international cooperation by the Special Prosecutor's Office in 2018 was particularly successful. The Office participated in the work of the Cross-Border Crime Group of the Council of Europe Convention on Cybercrime and in activities related to the preparation of further recommendations and guidelines for the application of the Convention. The Office also took part in the work of the Group drafting the second additional protocol to the Convention. The Office was further included in the Council of Europe and European Union joint project GLACY+, and in other international activities. In 2018, representatives of the Special Prosecutor's Office participated in the Council of Europe project EAP III, which was directed towards the so-called "neighbourhood" of the European Union, as well as in Cyber@South project, targeting the countries of North and West Africa and Asia in the Mediterranean Sea, and project iPROCEEDS@IPA, in which countries of South-Eastern Europe and Turkey were included. The European Judicial Cybercrime Network invited the Special Prosecutor's Office to participate in its meetings in the Hague. Representatives of the Special Prosecutor's Office also participated in the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime.

Singapore

312. Singapore referred to the challenges that it faced, which were common to other jurisdictions. These include the increased sophistication of criminals who seek to exploit the greater accessibility resulting from globalization and the advent and pervasiveness of technology to pursue criminal ends.

313. Singapore reported that the use of cyberspace had grown tremendously over the past decade. This is fuelled by cheaper and more accessible technology, which has led to an increase in the number of cybercrime cases (offences under the country's Computer Misuse Act, as well as offences where computing devices or networks are used as instruments to commit traditional crime). In this regard, the Singapore Police Force has seen an increase in the number of online scams and victims falling prey to new tactics employed by international scammers who make use of information and communications technologies, from high-end methods such as hacking to the use of call-spoofing technology. Owing to the reach and extensiveness of cyber-enabled crime across jurisdictions, such crime can take root anywhere, and is harder to detect, uproot and remove. Singapore has undertaken efforts nationally, regionally and internationally, detailed below, to tackle this complex challenge.

314. With regard to national efforts, Singapore reported that, on 20 July 2016, the Minister for Home Affairs and Minister for Law had announced the National Cybercrime Action Plan of Singapore at the RSA Conference, Asia-Pacific and Japan. The vision of the National Cybercrime Action Plan is to ensure a safe and secure online environment for Singapore as the activities of cybercriminals continue to grow in scale, complexity and severity worldwide. The Plan details the Government's multi-pronged strategy to combat cybercrime by:

(a) Educating and empowering the public to stay safe in cyberspace;

(b) Enhancing its capacity and capability to combat cybercrime;

(c) Strengthening legislation and the criminal justice framework;

(d) Stepping up partnerships and international engagements.

315. In terms of regional and international efforts, Singapore noted the useful role that international and regional organizations and multi-stakeholder partnerships played in capacity-building, fostering information, sharing the latest trends and developments, best practices and international cooperation in the fight against transboundary cybercrime.

316. Key regional platforms include the ASEAN Ministers' Meeting on Transnational Crime and the Senior Officials Meeting on Transnational Crime. As the ASEAN Voluntary Lead Shepherd for Cybercrime, Singapore has introduced new initiatives

to increase the response capabilities of ASEAN member States against cybercrime, such as hosting the ASEAN Plus Three Cybercrime Conference and the fifth ASEAN Senior Officials Roundtable on Cybercrime, in July 2018. ASEAN has also focused efforts at building up prosecutors' knowledge and capabilities in prosecuting cybercrime cases, and the ASEAN Cybercrime Prosecutors' Roundtable Meeting was held in Singapore in September 2018. These are annual events which will also be organized in 2019.

317. Singapore reported that it worked closely with INTERPOL to advance regional and international cooperation to combat cybercrime. Singapore was appointed as the Vice-Chair of the INTERPOL Eurasian Working Group on Cybercrime from 2017 to 2019. In addition, Singapore, with the support of INTERPOL, initiated the ASEAN Desk on Cybercrime, which was launched in July 2018 at the INTERPOL Global Complex for Innovation, located in Singapore. This ASEAN Desk taps into INTERPOL resources to drive ASEAN-centric joint operations against cybercrime. Singapore also participated in Operation ASEAN Cyber Surge, led by the INTERPOL Global Complex for Innovation in February 2017. The highly successful operation involved seven ASEAN countries and seven private sector companies and identified nearly 9,000 compromised servers and hundreds of malware-infected websites.

318. Additionally, Singapore is a supporting partner of INTERPOL World, an international conference held biennially in Singapore at which the public and private sectors gather to engage in dialogue and create collaborative opportunities to counter future security and policing challenges. This unique event provides a valuable platform for relevant stakeholders to discuss global cybercrime challenges and be updated by experts on the latest threats, trends and solutions.

319. Singapore has also actively participated in cross-jurisdiction international cybercrime enforcement operations. Singapore participated in Operation Avalanche, which was spearheaded by the United States Federal Bureau of Investigation, Europol and German Federal Criminal Police Office (BKA) in 2016 and again in 2017. The operation aimed to take down a global botnet used by a criminal network to steal bank account information and personal identity information and conduct money-laundering activities, as well as Andromeda, one of the longest-running malware systems in existence. Singapore also actively participates in international platforms focused on elevating global cooperation and exchange of best practices in the law enforcement domain. These platforms include the first UNODC National Cybercrime Roundtable Discussion, held in Indonesia on 2 and 3 July 2018, the UNODC Cryptocurrencies Experts Workshop held in Singapore from 12 to 14 March 2019 and the INTERPOL Global Cybercrime Expert Group Meeting and INTERPOL-Europol Cybercrime Conference.

320. Singapore concluded that the challenges faced by Member States in countering the use of information and communications technologies for criminal purposes were multi-pronged. Cybercrime is clearly an issue which will benefit from further discussion and strengthened international cooperation and collaboration at the regional and international level among Member States and relevant stakeholders, including at the United Nations. Singapore is committed to international and regional cooperation against cybercrime, and looks forward to participating, where possible, in capacity-building efforts. Furthermore, Singapore will continue to support collaboration and information-sharing to combat these challenges.

Slovakia

321. Slovakia reported that it paid great attention to the fight against cybercrime and considered the fight to be an important challenge. To effectively tackle the issue of cybercrime, two primary aspects must be met: legal and technical. Firstly, it is necessary to have adequate domestic legislation in place. Substantive criminal law provisions must be supplemented by appropriate procedural ones. Slovakia considered it important to ensure that traditional procedural provisions such as house

searches and surrendering, seizing or confiscating an object are extended to cover also data from a seized medium. Hence, with respect to the search of computer data, additional procedural provisions are necessary to ensure that computer data can be lawfully obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. Based on this, it is a must for domestic laws to contain provisions which allow State authorities to search and seize stored computer data. It must be ensured that all States have adequate provisions in place to prevent perpetrators of crimes hiding to avoid justice.

322. For Slovakia, a perfect example of a model containing a wide range of procedural powers is the Council of Europe Convention on Cybercrime, which provides, inter alia, for provisions on search and seizure, orders for computer data and data preservation. Slovakia ratified that Convention in 2008 and considers it to be the best international standard containing appropriate substantive and procedural provisions and allowing effective international cooperation. In the light of the above, for Slovakia, the successful implementation of the procedural powers contained in the Council of Europe Convention on Cybercrime, as well as a clear political willingness, are key factors to have in place a robust framework for securing evidence.

323. Furthermore, Slovakia was of the view that the importance of article 18, para. 1 (a) of the Council of Europe Convention on Cybercrime, which provides for the issuance of production orders, was that it really stood the test of time. The key element is not the location of data, but the presence of a controller or holder of data in a specific territory. This approach provides solutions in most cases, even in the age of cloud computing. Based on the above, Slovakia does not see the need for development of a new international instrument on cybercrime and encourages countries that are not parties to the Council of Europe Convention on Cybercrime to accede to it.

324. Slovakia further noted that almost every criminal offence might produce electronic evidence. The Council of Europe Convention on Cybercrime allows for gathering electronic evidence for all types of crime, which makes this instrument even more important. It follows from this that every judge or prosecutor should be made aware of how to use available means of securing electronic evidence. Educational activities and capacity-building programmes at the national and international levels in this respect are considered essential. According to Slovakia, capacity-building programmes must be targeted and, if possible, their duplication must be avoided.

325. Slovakia also referred to technical aspects, in addition to the legal ones. States should bear in mind that a key factor for successful cybercrime and cyber-enabled crime investigations lies in different kinds of specialization (local networks of prosecutors, judges on cybercrime, specialized judicial authorities on cybercrime, etc.), as well as regular training for law enforcement and judicial authorities to ensure that procedural powers are applied correctly and react to current developments. Networking and the exchange of best practices are necessary within States and at the international level.

326. To ensure that there is specialization and the continuous updating of expertise, Slovakia has established a special Computer Crime Department within the Presidium of Police Force. This Department helps to more effectively combat computer crimes and crimes committed over the Internet. The Department currently covers mainly cyberattacks on information systems, child sexual exploitation online, non-cash payment fraud and illegal online content (including terrorist content). Its tasks include seeking and monitoring cybercrime (including undercover Internet operations). It also provides cooperation to prosecutors when technical assistance is needed. The cooperation works very well. The Department also conducts dialogue with the international cybercrime police community, as well as with the private sector, especially Internet service providers, both in Slovakia and abroad, since the data of individuals are frequently in the possession or control of private entities and it is necessary to discuss the complexities and challenges of cooperation.

327. Furthermore, the National Network of Prosecutors against Cybercrime was established in 2017. Its main tasks are to provide practical information and to share experiences among members of the Network and with other prosecutors concerning cybercrime, regarding both national cases and cases of international cooperation.

328. At the national level, a multidisciplinary group of experts on cybercrime was established. It brings together experts from all important State authorities and the private sector. It holds discussions on, inter alia, how to modify the laws related to disclosure of data for criminal proceedings so that no court order is needed (in Slovakia, a court order is required to determine the user of a telephone number or IP address). Slovakia, thus, considers the establishment of specialized networks at the national and international levels that bring together practitioners dealing with cybercrime as beneficial.

329. Slovakia underlined that it was committed to the fight against cybercrime. Owing to the global nature of cybercrime, Slovakia confirmed that it very much appreciated the possibility to participate in the Expert Group to Conduct a Comprehensive Study on Cybercrime. Sharing best practices and exchanging views with experts from all over the world within the framework of this Expert Group is very useful and the Expert Group should remain the main process at the level of the United Nations on the topic of cybercrime until at least 2021.

Slovenia

330. Slovenia acknowledged that, with the rapid development of information technology, new services, equipment and devices were coming onto the market, along with new modus operandi for criminals. This requires rapid and adequate adaptation on the part of law enforcement authorities, which can only be ensured if there is effective and close cooperation with the private sector and research entities. Such cooperation entails secure and fast exchange of information, know-how, investigative techniques and methods, as well as ongoing training of personnel. Given the trends, an increase in criminal offences committed using modern, digital and virtual information or other technologies is to be expected.

331. The Slovenian police have noticed that perpetrators of criminal offences in cyberspace are becoming increasingly technologically skilled and well organized; they operate internationally and leave fewer usable traces and evidence that could make their identification easier. It all happens very fast, the number of victims is growing and restoring normality takes much longer. The traces left are, for the most part, only in digital form and frequently dispersed across several countries or continents, which adversely affects the duration and success of criminal investigations. Another challenge reported by Slovenia was the ever-increasing amount of data to be examined and analysed in each investigation, as well as the fact that strong data encryption was used by default by more e-device manufacturers. This gives criminals a high level of discretion and makes detection and prevention much more difficult.

332. Owing to the development and exploitation of technological achievements, the international environment faces challenges that can only be defeated through enhanced cooperation and reciprocity in the development of new practices for preventing and limiting risks, developing new approaches, tools and mechanisms and through more reciprocal action and solidarity in prevention at the operation level. The international dispersion of evidence and operation of perpetrators would require the introduction of new investigative forms, better legislation and improved qualification and equipment.

South Africa

333. Referring to challenges related to existing instruments of legal and criminal law for the use of information and communications technologies, South Africa reported

that it had legislation to combat acts of cybercrime, which included the Cybercrimes Bill (soon to be an Act of Parliament), the Criminal Procedure Act, the Electronic Communications and Transactions Act, the International Cooperation in Criminal Matters Act and the Protection of Personal Information Act. Further, South Africa stated that the lack of international consensus on key issues and concepts, including the nature and dimensions of cyberthreats, the fairness of procedures and outcomes of formal frameworks and the criminalization of specific conducts as cybercrime presented challenges in combating the use of information and communications technologies for criminal purposes. These challenges extend beyond definitional elements, which vary substantially.

334. South Africa also referred to the coordination and cooperation among States in combating the use of information and communications technologies for criminal purposes. Despite the availability of a number of existing mechanisms to promote coordination and cooperation, such as mutual legal assistance, designated points of contact, obligations on electronic communications service providers and financial institutions, as well as expedited disclosure of traffic data by various service providers, there remain challenges in addressing cybercrime. The following were identified as challenges of significance: the lengthy mutual legal assistance process; different agencies having different mandates, which make central coordination difficult; and the coordination mechanism and the implementation of proposed measures which are not fully supported by various stakeholders. While existing regional instruments may work in addressing cyberthreats by enabling cooperation among those who are parties to conventions, the biggest challenge is that they may not effectively combat cybercrime globally, as States that are not parties to the Convention may not cooperate. The absence of a universally agreed definition of cybercrime poses a challenge and therefore each country has developed its own definition, resulting in challenges when it comes to mutual legal assistance or international cooperation, including extradition and sharing of electronic evidence. In order to effectively implement laws on cybercrime and, in particular, where there is a need for cooperation with other States, it is important to ensure that there is some harmonization of laws, which would require an agreement on the definition of cybercrime. Various binding or non-binding regional instruments exist that aim to deal with cybercrime but many countries, because of their political dispensations, international agendas and socioeconomic circumstances, may not want to ratify any of the existent regional instruments.

335. In terms of technical assistance, South Africa noted that, while bilateral and multilateral agreements (e.g., Organized Crime Convention provisions on mutual legal assistance, extradition, transfer of sentenced prisoners and asset confiscation) exist, regional and continental agreements seem to supersede them in terms of functionality. International cooperation relating to cybercrime is in most instances limited and does not include the necessary procedures to, among others, preserve evidence, make traffic data available on an expedited basis or ensure the availability of evidence.

336. Other challenges which, in the view of South Africa, remain are the varying national laws of countries that include different descriptions of cybercrime; the different procedures relating to international cooperation; formal country-to-country procedures that must be followed before evidence is admissible before courts; privacy laws; and so forth.

337. For South Africa, the lack of national structures in various countries with coordination powers to coordinate mutual assistance requests hampers the effectiveness of mutual legal assistance. Various regional instruments that are aimed at addressing cybercrime lead to fragmentation and silo-based cooperation between countries and are unsuccessful in assuring adequate international cooperation. The absence of a universally recognized instrument at the United Nations level that deals with international cooperation in cybercrime matters is a significant contributing factor to the ineffectiveness of international cooperation in this field.

338. South Africa is convinced that the role of UNODC and, in particular, the Commission on Crime Prevention and Criminal Justice in providing capacity-building should be enhanced. The fact that various national authorities lack funding for specialized training to enable them to effectively investigate complex cybercrime cases is a problem. Likewise, the retention of experienced and trained officers is difficult owing to demand in the private sector. There is a widespread lack of basic and intermediate training programmes in law enforcement training institutions, and experienced investigators, because of their workload, are seldom afforded the opportunity to attend advanced training courses or workshops. Even with the best intentions and proposed measures, budget and capacity constraints make it difficult to implement proposed measures and available capacity and resources are often restricted to the mandate of an agency and cannot necessarily be used to assist other agencies. Furthermore, no formal frameworks or guidelines exist for cooperation among relevant stakeholders in the area of cybercrime.

Spain

339. Spain reported that cybercrime resulting from the growing use of information and communications technologies was one of the main threats and one of the most important challenges faced by all States, also because of the diversification of the criminal methodologies employed by transnational organized groups. Criminals make use of communication platforms and new information and communications technologies to create new illegal business models such as the use of the darknet to enable the commission of other crimes (such as trafficking in firearms and counterfeit money), the use of sophisticated malwares (such as ransomware) and bank infrastructure controller and the so-called “individual criminal entrepreneur”, who offers illicit services. All the above constitute challenges to security officials and to society at large.

340. The widespread and rapid growth of Internet access and the increased number of devices that provide connectivity will lead to an increase in the number of potential victims of cybercrime. Likewise, bearing in mind the growing population rate in developing countries (primarily in Africa) and the estimates of the growth in the number of Internet users in those countries, it is easy to anticipate a significant increase in the use of the Internet for committing crimes, specifically economic crimes. However, in the same way that criminals learn how to make use of the new technologies to develop new modi operandi, police authorities could also make use of technological innovation and develop new measures to investigate and combat the threat posed by organized and serious crime.

341. The inclusion in national law of requirements for undercover investigations on the Internet was considered by Spain as a key tool in the fight against organized and serious crimes which are committed through the use of information and communications technologies. That is also the case with the progressive use of new technologies, such as drones, specifically directed software, cloud services and rapid access to social networks.

342. In Spain, measures against crimes planned and carried out over the Internet, and in general through information and communications technologies, constitute an important part of the National Security Strategy, published in December 2013 and currently being updated. As a result, the fight against cybercrime is considered part of a broader objective to make the use of cyberspace safe, on the basis of on an integrated model. This includes coordination and cooperation among the public administration, the private sector and citizens and, at the same time, integrating international initiatives into the internal and international legal order. This approach has been realized in different ways.

343. First, in terms of legislative reforms, in 2015, Organic Laws 1/2015 and 2/2015 brought about an important reform of the Spanish Penal Code, inspired by European regulations (directive 2013/40 and directive 2011/93, DM 2008/919/JAI, etc.) and by

the Council of Europe Convention on Cybercrime and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. These instruments include definitions of new crimes, which inspired extensive reform of related provisions of the Penal Code such as those on computer attacks, sexual harassment of minors, child pornography, intellectual property, hate crimes, computer fraud and terrorism offences. Also in 2015, through Organic Law 13/2015, a meaningful reform of the Law of Criminal Procedure, inspired by the Council of Europe Convention on Cybercrime, was adopted. It regulated important technological measures related to the registration, storing and preservation of data. To facilitate the interpretation of these legislative developments, the State Attorney General's Office published relevant circulars.

344. Second, in relation to organizational measures, all national and autonomous police corps in Spain have had, for more than 20 years, specialized units composed of staff who are highly qualified in technological research, with knowledge and experience to effectively counter the use of information and communications technologies for criminal purposes. This expertise allows police authorities to make use of new technologies, such as big data, as well as web-based devices that can be inserted in products such as clothes, jewellery and shoes to investigate crimes and identify suspects.

345. The Spanish Public Prosecutor's Office has also created specialization in the area of cybercrime. Since 2011, the national network of prosecutors dedicated specifically to the prosecution of cybercrimes has deployed approximately 150 prosecutors across the national territory, in the 50 provincial capitals and in a number of selected cities. The specialized units of the Prosecutor's Office and the Police maintain constant contact with other bodies with responsibility for cybersecurity in order to ensure adequate coordination and to make the use of cyberspace safe to all. These include the Spanish Agency for Data Protection, the National Centre for the Protection of Critical Infrastructure, the National Institute of Cybersecurity, the National Cryptological Centre and the Joint Cyber Defence Command, and private sector organizations and entities such as banking entities or those in charge of telecommunications and other essential services.

346. Spain considered it important to continue supporting the training of specialized units against cybercrime, as well as to increase their human and material resources. The training of researchers and legal officers, mainly judges and prosecutors, had also received attention in recent years and was presented at two levels:

(a) Generic preparation on basic and essential knowledge, delivered to all professionals involved in the fight against crime;

(b) Specialized training for units or groups that deal specifically with cybercrime.

347. Spain stated that international cooperation was important in responding to the common challenge of cybercrime for all States. Some examples of the country's participation in international cooperation efforts included active participation in the 24/7 Network established in article 35 of the Council of Europe Convention on Cybercrime; in the European Judicial Network against Cybercrime; and in the European Network of Intellectual Property Specialist Prosecutors. Similarly, the Spanish Public Prosecutor's Office promotes and participates in the Ibero-American network of specialist prosecutors (CibeRed).

348. Spain reported that it is an active member of the Cybercrime Convention Committee of the Council of Europe Convention on Cybercrime and of the working groups for the preparation of its second additional protocol, aimed at improving international cooperation and collaboration with operators, suppliers and entities in the private sector. Spain participates in numerous transnational investigations, with both European and Latin American countries, using advanced cooperation techniques such as joint investigation teams. It also participates in training in other countries, including as trainer.

Sri Lanka

349. Sri Lanka emphasized that it had been actively participating in the Expert Group to Conduct a Comprehensive Study on Cybercrime, which had recently reviewed chapters 5 and 6 of the draft comprehensive study on cybercrime from February 2013. At its next meeting, the Expert Group would focus on the final two chapters, 7 and 8 (International cooperation and Prevention).

350. Sri Lanka wished to clarify the link between the information sought through General Assembly resolution 73/187 and the ongoing work at UNODC on the draft comprehensive study on cybercrime, and whether the work of the Expert Group to Conduct a Comprehensive Study on Cybercrime was being duplicated.

351. In terms of domestic legislation on cybercrime, Sri Lanka reported that the Computer Crimes Act No. 24 of 2007 was the primary legislative tool in the fight against cybercrime. In addition, the Payment Devices Frauds Act No. 30 of 2006 specifically deals with possession or use of unauthorized or counterfeit payment devices.

352. Sri Lanka became a State party to the Council of Europe Convention on Cybercrime in 2015. As such, it has demonstrated a strong commitment to harmonize and improve national laws in accordance with the best available international standards governing the fight against cybercrime. Sri Lanka is also committed to improving investigative techniques and enhancing the ability of criminal justice officials to adopt more effective enforcement techniques.

353. While the substantive law provisions embodied in sections 3–10 of the Computer Crimes Act are based on articles 2–8 of the Council of Europe Convention on Cybercrime, article 9 is partly reflected in section 286A of the Penal Code (Amendment) Act No. 22 of 1995. The Intellectual Property Act No. 36 of 2003 deals with offences covered in article 10 of the Council of Europe Convention on Cybercrime.

354. In order to address evolving cybercrime challenges, Sri Lanka has embarked on a review of national criminal justice measures in the area of online child safety. Consequently, Sri Lanka recently approved an Amendment to the Obscene Publications Ordinance to comprehensively deal with child pornography-related offences. A new chapter entitled “Child pornography through the use of computer systems” will be introduced through this amendment.

355. In terms of enforcement measures related to cybercrime and electronic evidence, the procedural provisions contained in part II of the Computer Crimes Act provide for interception, real-time collection of basic subscriber information and traffic data and the making of preservation requests. Such provisions are subject to safeguards consistent with article 15 of the Council of Europe Convention on Cybercrime.[9]

356. Under section 18 of the Act, a warrant issued by a magistrate is required by law enforcement agencies to obtain basic subscriber information in the possession of service providers. A similar requirement has to be fulfilled for the interception of communications. Data preservation orders under section 19 of the Act require any person in charge of a computer or an information system to preserve data at the request of law enforcement agencies. However, the duration is restricted to a period of seven days. An extension of the preservation period can be secured only through a court order.

[9] Under the Computer Crimes Act, intrusive investigative measures such as search and seizure of computers or the interception of a communication are subject to a warrant by a magistrate (section 18). The Constitution of Sri Lanka stipulates and guarantees several fundamental rights in chapter III. Sri Lanka is also party to a number of international human rights treaties such as the International Covenant on Economic, Social and Cultural Rights, the International Covenant on Civil and Political Rights, the Convention on the Rights of the Child and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

357. Judicial oversight of these procedural measures protects the service providers from unnecessary and arbitrary requests from law enforcement agencies while ensuring that they assist law enforcement officers to combat crime effectively. These safeguards in national legislation have not adversely affected the efficiency or the effectiveness of criminal investigations. On the other hand, they have created greater confidence for victims and businesses (especially banks and financial sector organizations) to report incidents of cybercrime and have also created confidence among telecommunications service providers with regard to cooperating with law enforcement agencies. This could be noted as a best practice for developing countries.

358. Within the police, a specialized cybercrime investigations unit has been established, with two provincial branches. This functions as the 24/7 contact point under the Council of Europe Convention on Cybercrime. It was upgraded recently and over 750 cases have been successfully investigated with the expertise that national officials have gained through the capacity-building measures mentioned below.

359. Sri Lanka stressed that securing electronic evidence from foreign service providers was vital for the investigation and prosecution of cybercrime offences. Since evidence is located in different jurisdictions, the need for more effective investigative methods, coupled with effective international cooperation measures, is paramount. International cooperation in criminal justice matters is dealt with under the Mutual Assistance in Criminal Matters Act No. 25 of 2002. This Act has been incorporated by reference into the Computer Crimes Act and Act 25 of 2002 was amended in 2018, by Act No. 24 of 2018, with features of the Council of Europe Convention on Cybercrime.

360. In terms of capacity-building measures, a series of programmes on cybercrime and electronic evidence, covering the judiciary, the Attorney General's Department and police units, have focused on enhancing enforcement and investigation methods. These are carried out under a project supported by the European Union and the Council of Europe. Such capacity-building measures have enhanced the ability of national law enforcement officials to adopt more effective standard operating procedures on the basis of good practices and experiences, as well as lessons learned from other States parties to the Council of Europe Convention on Cybercrime.

361. Sri Lanka reported that the Government had adopted a comprehensive cybersecurity strategy in October 2018. Consequently, Sri Lanka is now drafting cybersecurity and data protection legislation. These initiatives are led by the Ministry of Digital Infrastructure and Information Technology, supported by computer emergency response teams, the Information and Communications Technology Agency, the Central Bank of Sri Lanka and other key stakeholders. The Ministry has included the private sector in these efforts and the Government will follow an inclusive approach by consulting key stakeholders in the review of new draft legislation.

Switzerland

362. Switzerland noted that the evolution of information and communications technologies, while offering unprecedented opportunities for individuals, corporations, businesses and commerce, also presented challenges, particularly in the area of criminal justice and therefore the rule of law. While cybercrime in the strict sense of the term, i.e., offences committed through computer systems, including offences that leave electronic evidence on computer systems, is developing, and while evidence of such offences is increasingly stored on servers located in foreign jurisdictions, which may be multiple, changing or unknown, for example in the cloud, law enforcement authorities are limited by territorial boundaries and must respect the sovereignty of States.

363. Switzerland noted with concern the limited effectiveness of mutual legal assistance in securing volatile electronic evidence, situations of loss of (knowledge

of) data localization and the fact that States were increasingly relying on unilateral cross-border access to data in the absence of international rules.

364. As a State party to the Council of Europe Convention on Cybercrime, Switzerland stressed its importance. For Switzerland, the Convention greatly facilitates cooperation by harmonizing laws, establishing procedures and designating points of contact. On the basis of that Convention, it is necessary to facilitate and increase international cooperation.

365. The question of whether a service provider is sufficiently present or offers a service in the territory of a State party, thus being subject to the jurisdiction of that State, will be crucial in the years to come. The question will be relevant not only in terms of criminal law, but also in terms of tax and copyright law, for example.

366. Switzerland underlined that States' obligations under international law, in particular human rights law, must be observed at all times, including when regulating cyberspace and when criminalizing, investigating and prosecuting cybercrime. The principles of data protection and other rule-of-law safeguards must be kept in mind and followed, in particular when new ways of international cooperation and transnational investigations are being examined and discussed.

Syrian Arab Republic

367. The Syrian Arab Republic underscored that the threat of cybercrime was increasing day by day as the use of information and communications technologies by criminal networks and terrorist groups to achieve their criminal and terrorist purposes also increased. This affects the stability of countries, their infrastructure and institutions, especially the social and cultural fabric and economic development and developmental advancement. The widening of the digital divide between States inevitably undermines the ability of many States to prevent, prosecute and combat such crimes.

368. According to the Syrian Arab Republic, there is no doubt that the high rates of crime and the increase in the number of crimes committed in the digital world have had a significant impact on the spread of terrorist crimes around the world, especially those committed by terrorist organization in Iraq and the Syrian Arab Republic. The uncontrolled and untraceable digital space facilitates terrorists in the commission of all forms of crime, from murder, trafficking in persons, trafficking in cultural property and the looting of religious monuments and sites to the use of the Internet for child abuse, abduction and recruitment for use in hostilities and terrorism, acts of racism and incitement to hatred and sectarian, ethnic or doctrine-based strife, as well as other grave violations of relevant international laws, conventions and resolutions that require serious international response.

369. The Syrian Arab Republic has taken numerous measures to address the threat of cybercrime and the use of digital space by terrorist groups to commit the most heinous forms of transnational terrorist crimes, including through the strengthening of legal frameworks. In this regard, the Government issued Legislative Decree No. 17 of 2012 on combating cybercrime and the enactment of the Digital Criminal Code to increase the effectiveness of combating traditional crimes involving the use of information and communications technologies. Law No. 9 of 2018, which includes the creation of a public prosecution and specialized courts for information and communications crimes, has been established to increase awareness of the seriousness of this crime and to build capacity and protect victims in the country.

370. In the practical application of legislation, the competent authorities have faced many problems and challenges, considering that this type of crime has no limits in nature and thus makes criminal investigations more complicated for law enforcement authorities. These challenges include confronting the monopoly of developed countries on the global Internet; and the politicization of work and lack of cooperation in the area of sharing with the authorities of the Syrian Arab Republic evidence and

information about persons who commit criminal activities over the Internet. In addition, the Syrian Arab Republic reported that the blockade and the unilateral and illegal coercive measures imposed on it by the United States and other countries and the European Union that have a monopoly over communications technologies have limited the access of the relevant authorities of the country to the technologies and tools necessary to combat these criminal activities.

371. For the Syrian Arab Republic, the criminal law legal instruments currently used at the international and regional levels are insufficient to counter the illegal use of information and communications technologies in criminal and terrorist operations. Currently, there is no international convention in this context except for the Council of Europe Convention on Cybercrime, which does not cover the use of information technology in terrorist acts.

372. In the light of the above and in order to enhance the fight against the use of information and communications technologies for criminal purposes, the Syrian Arab Republic recommended the following:

(a) States adhering strictly to their international obligations and the implementation of relevant Security Council resolutions against terrorism;

(b) Promoting effective regional and international cooperation, including through the exchange of information, and developing an agreed flexible mechanism to exchange information and digital evidence;

(c) Reaching a preliminary agreement among Member States on ways to examine solutions in the fight against crimes committed using information and communications technologies to allow for the establishment of an open-ended United Nations working group in New York to ensure the participation of all States concerned in the discussion of this subject;

(d) Developing a binding international legal instrument on international cooperation in this area consistent with the interests of Member States, taking into account that existing criminal law legal instruments are not sufficient to combat information and communications technologies crime;

(e) Bridging the “digital divide” through the abandonment by States of their monopoly on electronic technology and its tools after it has proved unable to fully protect against the consequences of the misuse of information and communications technologies by lifting restrictions on the transfer of technology and tools to all countries without discrimination;

(f) Strengthening prevention and protection measures through cooperation and the active participation of all States;

(g) Speeding up responses to requests for international cooperation, especially for the purpose of securing and maintaining digital evidence and setting time frames for such response;

(h) Considering the establishment of an interactive global online platform which includes the relevant national authorities from each Member State. The platform would facilitate information-sharing on transnational cybercrime cases and would offer guidelines on the safe use of online databases in addition to offering specialized programmes to help prevent cybercriminality and membership in cybercriminality, as well as other guidelines that ensure swift responses to match the complexity of the technology used in such crimes;

(i) Building national capacities and technical assistance to improve the skills of competent authorities to effectively address cybercrime challenges and challenges associated with digital evidence, including by supporting national efforts to develop and deploy Internet infrastructure to improve cybercrime capabilities and supporting training and awareness on technical issues and digitization of record-keeping;

(j) Having in place the necessary equipment to obtain digital evidence and support the training of a sufficient number of qualified and trained digital

investigators in cybercrime verification techniques and the extraction of related digital evidence;

(k) Establishing binding regulatory standards on the use of digital space, taking into account the balancing of Internet freedom, privacy and the security of States, as well as developing frameworks to counter the abuse of the digital space. For example, the placement of currency exchange sites bitcoin that could be used for money-laundering and terrorist financing and social networking platforms used to incite crimes under surveillance;

(l) Strengthening the partnership between the concerned government agencies and private sector companies such as Internet service providers, cellular networks and others to make available the information stored on demand, in accordance with legal and judicial controls, to complete the investigation of information crimes and extract evidence.

Tajikistan

373. Tajikistan noted that the spread of information and communications technologies and the development of the information infrastructure had contributed to the creation of the information society. As world practice shows, the information age has expanded the mechanisms of political violence, adding to the physical methods of persuasion, manipulation of consciousness and other informational ways of influencing public consciousness.

374. Tajikistan made the following recommendations:

(a) Governments should be encouraged to provide adequate information and professional training for their law enforcement personnel and provide them with adequate resources to effectively investigate crimes related to the use of the Internet and other information and communications technologies;

(b) Governments should encourage their law enforcement authorities to acquire specialized skills that will facilitate the investigation of cybercrime and allow them to successfully conduct criminal investigations;

(c) Governments must act collectively to ensure effective inter-agency and interregional information exchange, remove obstacles encountered in conducting investigations on cybercrime in a few countries and make the necessary changes to legislation, practices and procedures in order to accelerate the exchange of information, the processing of requests from various information resources and the transfer of digital evidence;

(d) It is necessary to organize regular specific courses and ensure proper professional training of employees of law enforcement authorities in the fight against cybercrime and the use of the Internet and other information and communications technologies;

(e) It is considered necessary to develop and adopt a universal United Nations convention on cooperation in the fight against crimes related to the use of information and communications technologies, which would be in the interests of all Member States.

Thailand

375. Thailand reported that typical cybercrime offences encountered in the country included hacking, Internet fraud, intrusion, cyberstalking, online identity theft, online child abuse, abusive content, malicious code and ransomware attacks. Criminals always seek gaps in technology to conceal their identity, including through innovative approaches such as using decryption currency (cryptocurrency) in the blockchain system for money-laundering.

376. Thailand also reported that the difficulty of collecting digital evidence was encountered in most cybercrime cases. This is due to the fact that important evidence in cybercrime prosecution lies in computer traffic data held by Internet service providers and social media service providers such as Facebook, Line, Instagram, WeChat and WhatsApp, which are often registered in foreign countries and not compelled to render assistance and cooperation in accordance with the Computer-Related Crime Act of Thailand. Therefore, law enforcement agencies may need to acquire such evidence through the formal channel of mutual legal assistance treaties. This process consumes a long period of time and may become difficult in practice. The information obtained through informal cooperation channels, although helpful, may be inappropriate as evidence before a court.

377. In addition, some new technologies, such as encryption, prevent access to data. Some "smart" mobile telephones may not be unlocked without the consent of the devices' owners, thus preventing access to their operating systems. In addition, a lack of digital forensic tools and software because of their high cost is a common problem faced by computer forensic examiners; free tools and open-source software have limited capabilities in computer forensic examination.

378. Thailand also reported that law enforcement agencies might have insufficient understanding about digital evidence and modern financial banking technologies. Many officers may lack experiences in reading financial statements or seeking circumstantial evidence, including through modern cyber-investigative techniques. Cybercrime training for public prosecutors and other law enforcement officers and a platform to share knowledge and best practices are thus needed.

379. Although the Computer-Related Crime Act imposes a duty on service providers to maintain traffic data and provide requested information to a competent authority, some service providers do not always fully comply. Some take time to render the requested data because of a large number of requests. Some are reluctant to disclose data because of their concerns over customer privacy.

380. Thailand underlined that the increasing use of information and communications technologies and, with it, access of a higher number of devices to Internet services have put the critical infrastructure of States and enterprises at risk. While these devices are possibly affected and compromised in technological terms, the information system has to remain stable and fully secure. Collaboration among all concerned agencies and all stakeholders is needed to protect the system. It is also difficult to clearly identify the intention of requests received by service providers.

381. In Thailand, the Computer-Related Crime Act B.E.2550 (2007) serves as the key law in dealing with cybercrime prosecution. It is used in conjunction with other laws that impose criminal offences related to cybercrime such as the Criminal Code, the Anti-Trafficking in Persons Act, the Narcotics Act, the Copyright Act and the Prevention and Suppression of Involvement in Transnational Criminal Organization Act. The promulgation of relevant laws has to come with capacity-building programmes for officers at the working level, including law enforcement officers, as well as effective coordination mechanisms. There is an urgent need to raise digital literacy and the awareness and understanding of stakeholders and prepare them for the implementation of such laws.

382. In relation to the protection of the rights of individuals, including children, Thailand reported that those involved in trafficking in persons, cyberbullying and Internet frauds, including scams, had made use of new technologies to communicate directly with individuals and gain their trust for criminal purposes. At the same time, extreme and negative ideologies are increasingly disseminated over the Internet. The key challenges include:

(a) The effective implementation of laws and regulations that are in place;

(b) Coordination among concerned agencies such as law enforcement officers, financial operators and stakeholders;

(c) Multi-stakeholder engagement in promoting and protecting the rights of individuals.

383. In the view of Thailand, the investigation of related crimes has to take into account victims' feelings and circumstances and, thus, require a context-specific human rights-based approach. Among those in vulnerable situations, children stand out as a target of cyberbullying, cyberstalking, Internet gaming, sexting, child sexual abuse material, online grooming and sextortion. Special attention should be paid to social media sites such as Facebook, Instagram and Twitter.

384. Thailand concluded that no country could prevent and suppress cybercrime alone. Therefore, international cooperation and dialogue among Member States are very important. Thailand has participated in the Expert Group to Conduct a Comprehensive Study on Cybercrime, which is the only platform in this matter. Thailand hopes that the Expert Group's mandate and work will be extended beyond 2021.

Turkey

385. Turkey underscored that information and communications technologies were used in a broad network that involved the public and private sectors, critical infrastructure and individuals, and became widespread both nationally and internationally. As a result of this, information and communications technologies play an important role in sustainable growth and development. However, the more that technology is used, the more society becomes dependent on it and subject to the risks it brings forth. Individuals, companies, critical infrastructure and States encounter serious problems because of cyberincidents. Security weaknesses in information and communications systems may cause such systems to become out of service or to be exploited, or may lead to an eventual loss of life, large-scale economic loss, disturbance of public order and/or compromises to national security. On the other hand, cyberspace provides advantages such as anonymity and deniability for attacks on information and communications technologies. It is hard to detect the financers and organizers of persistent and advanced cyberattacks targeting information systems. This situation makes it difficult fighting against threats and attackers.

386. Within this context, not only is cooperation at the national level, including stakeholders such as the public and private sectors, universities, non-governmental organizations and individuals crucial, but so is international cooperation and information-sharing. One of the main strategic aims of the National Cybersecurity Strategy and Action Plan was combating cybercrimes. In this respect, Turkey supports and contributes to activities at the international level within the concept of the fight against cybercrime.

387. Turkey signed the Council of Europe Convention on Cybercrime in 2010. The Convention was then incorporated into domestic law through the enactment of the Law on Approval of Ratification of the Convention on Cybercrime in 2014. In addition, cybersecurity-related issues are regulated in the Turkish Penal Code.

388. Turkey noted that, with the increasingly widespread use of the Internet and the ever-advancing information and communications technologies, cyberspace had become a hub of all things, attracting many kinds of hostile actors. The identification of cybercriminals has been getting increasingly harder because of the layered structure of Internet and the proxy servers used to access it. The malicious use of such technologies provides the necessary instruments for the commission of cybercrime offences and a convenient medium for communication by terrorist groups. Illegal organizations use information and communications technologies to promote and disseminate propaganda, collect information, raise funds, recruit new members, orchestrate organized activities, share information and plan or coordinate acts of terror. Terrorist groups tend to use applications and tools that offer encrypted channels to communicate or plan or coordinate their hostile acts. This situation makes it difficult for law enforcement entities to identify terrorists' identity and activities.

389. In the view of Turkey, strengthening information security at the global level and developing the security culture of the international community are crucial matters for every stakeholder. Strengthening international legislation and enhancing bilateral or multilateral international agreements is also important. In this respect, Turkey believes that developing measures which would facilitate the prevention of criminal use of information and communications technologies and strengthen international cooperation mechanisms in this field would contribute to identifying and thwarting terrorists and their activities.

390. On the other hand, illegal content published on the Internet can be considered as a serious problem that poses challenges to ensuring cybersecurity. Malicious attacks made by terrorist organizations against common humanitarian values and the right to live all over the world, as well as the content being broadcast over Internet as propaganda tools, underscore the importance of prevention of the use of Internet for illegal purposes. Within this context, combating illegal content on the Internet should be considered as a responsibility not only of States, but also of the global Internet companies that are the greatest actors on the Internet. Therefore, Internet actors should act in cooperation with the relevant States for the purpose of carefully preventing the criminal activities of all criminal organizations on their platforms.

391. In the view of Turkey, considering that all terrorist groups use cyberspace for criminal activities with different motivations, there is a strong need for global Internet intermediaries to respond as fast and sensitively as possible to requests for the removal of illegal content related to these terrorist groups. Robust and continuous implementation of decisions on the removal of content has great importance; otherwise, malicious use of the Internet by terrorist groups could result in irreversible harm. In this regard, relevant content and host providers' collaboration is vital to ensure full cooperation. The compliance of global providers with requests for content removal, in accordance with national and international legislation and judicial orders, will assist greatly in combating illegal content on online platforms.

United Kingdom of Great Britain and Northern Ireland

392. The United Kingdom stated that the concept of "use of information and communications technologies for criminal purposes" would be interpreted as self-explanatory for the purposes of its response (and wider in scope than cybercrime), although the broad framing of the question did not permit a straightforward answer. The challenges to tackling the use of information and communications technologies in crimes manifest in highly diverse and complex ways depending on a varied number of factors. These factors include the motivations of offenders, the corresponding profile and/or vulnerabilities of the victims, the method and technological means applied by the offenders, including specific methods to mask their activity, and, reflecting all of the above; whether the crime includes network or system intrusion or relates to criminal content (e.g., child sexual exploitation material).

393. Given these variations and the prevalence of information and communications technologies in all contemporary crime, either in the form of digital evidence or where the information and communications technology component represents a crime in its own right, the concept of "use of information and communications technologies for criminal purposes" is limited in diagnostic usefulness. The United Kingdom has observed that the "digital factor" in crime has been a reality for some time, reflecting both how criminals have mainstreamed the use of information and communications technologies to expand the scale of and opportunities for their offending and the increased use and reliance on the Internet throughout societies. The resulting challenges for law enforcement entities are thus arguably inseparable from some of the broad and myriad challenges that societies face in addressing many contemporary crimes in general.

394. Notwithstanding these definitional issues, the United Kingdom referred to a number of strategic challenges that are universal to Member States' abilities to

specifically investigate and resolve crimes with an information and communications technology component, including:

(a) Insufficient technical capabilities or capacity to conduct digital investigations, including a lack of staff with proficient information and communications technology skills, or difficulties in retaining such staff, particularly within domestic law enforcement agencies;

(b) The lack of domestic substantive laws in a number of jurisdictions to criminalize information and communications technology-related offences and serve as the basis for international cooperation through the mutual recognition of such offences (dual criminality);

(c) The lack of domestic procedural laws, with appropriate human rights safeguards and oversight regimes, to permit the investigation of information and communications technology-related offences and the admissibility of digital evidence in court;

(d) Challenges in measuring the scale and indirect impact of information and communications technology-related offences, and subsequent challenges in increasing the awareness of the public of their harms and encouraging the reporting of such offences;

(e) Challenges in encouraging public awareness and adoption of cybersecurity behaviours and/or awareness of information and communications technology-related crimes to reduce their vulnerability to such crimes, and/or to understand where criminality has occurred, for the purposes of reporting it;

(f) The general challenges arising from countries with weak rule of law, or non-cooperative jurisdictions harbouring cybercriminals, reflecting the cross-border nature of such crimes and the fact such crimes bypass the need for a physical footprint in the victim countries;

(g) As noted in the National Crime Agency's National Strategic Assessment 2018, the challenges arising from technological means used by criminals to more effectively mask their activities, including the use of technologies such as the darknet, encryption, virtual private networks and virtual currencies.

395. A number of the above-mentioned challenges that are particularly relevant to the United Kingdom have been outlined in the written submission to the fifth meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, on the topics of law enforcement and investigations and electronic evidence and criminal justice.[10]

396. Outside of these two topics, the challenge of underreporting of cyber-dependent crime remains a particular challenge. The United Kingdom has identified a known gap between public experiences of cybercrime and the reporting of it, through comparisons of public surveys and official crime reporting statistics.

397. The United Kingdom also faces challenges related to uncooperative jurisdictions. In the National Strategic Assessment 2018, the National Crime Agency noted that "cyber crime groups, many of which operate internationally and are Russian-speaking, continue to pose a threat to United Kingdom interests". In many cases, such groups are physically based in jurisdictions which do not permit extradition of citizens for such crimes, or where cooperation against such groups is not always forthcoming.

398. The United Kingdom believes that the Expert Group to Conduct a Comprehensive Study on Cybercrime offers a unique opportunity to continue to explore consensus-based solutions for tackling cybercrime among Member States. In particular, the Group's status as a platform for experts, and with a mandate to systematically consider a wide range of themes, is ideally suited to ensure discussions

[10] Available at www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

on responses to cybercrime take account of a comprehensive set of viewpoints and possible solutions. The United Kingdom therefore believes that it is important to ensure that the Expert Group process is recognized as the primary platform for cybercrime discussions under the auspices of the Commission on Crime Prevention and Criminal Justice, in keeping with the Commission's mandate to consider other crime-related matters. Furthermore, the United Kingdom encourages UNODC and Member States to take full advantage of the Expert Group, as a platform for technical discussions by experts, to guide the work of the UNODC technical assistance programme on cybercrime.

399. The United Kingdom also believes the Council of Europe Convention on Cybercrime is the most effective framework upon which to build further international consensus and harmonize approaches to cybercrime. With 63 parties, it has broad consensus across numerous regions and has proved itself compatible with diverse legal and institutional settings. Through the Cybercrime Convention Committee, which facilitates dialogue among parties to the Convention, the Convention also has robust mechanisms to ensure that it is able to take account of developments in the cybercrime space and keeps pace with new challenges and technologies. The United Kingdom therefore recommends that those Member States not already party to the Convention take steps to request accession, subject to ensuring that proper human rights safeguards and domestic procedural laws are in place. Where such domestic provisions are not already in place, the Council of Europe has programmes to build capacities for accession; the United Kingdom therefore believes that Member States should engage with the Council of Europe to determine the availability of such technical assistance programmes for such purposes, where appropriate.

United States of America

400. The United States reported that it faces four main challenges, the first being the pressure to limit expert input to international policy. While traditional law enforcement methods are adaptable to cybercrime, the challenges posed are complex and evolving. Thus, any United Nations policy debates on cybercrime should benefit from direct input and advice from technical experts. Pressure applied by some Governments to launch political debates on new global treaties, despite the lack of consensus support for such an approach, consumes valuable resources and undermines the ability of experts to provide meaningful advice on how to overcome core challenges faced by Member States when investigating and prosecuting cybercrime. The input of experts is essential to understand complex issues such as:

(a) The protection of freedom of expression;

(b) Appropriate limits on State authority;

(c) The effective implementation of existing frameworks and mechanisms;

(d) The timely delivery of training and technical assistance for developing countries.

401. This problem was demonstrated during the adoption of General Assembly resolution 73/187, where a split vote launched new General Assembly political debates in a manner that undermines the ability of the Expert Group to Conduct a Comprehensive Study on Cybercrime, established pursuant to General Assembly resolution 65/230, to carry out its mandate. Resolution 73/187 hinders the efforts of the Expert Group by creating another report before the Expert Group's own workplan is completed, and advances that report in a venue in which law enforcement experts do not typically participate. Member States should bolster the input and participation of law enforcement and criminal justice experts, private industry and civil society in United Nations policy-making processes. Member States should also ensure that policy debates are organized on the basis of the advice of national experts, who are on the "front line" in combating cybercrime.

402. The second challenge is related to the evolution of cybercrime and transnational criminal organizations. Transnational criminal organizations have broadened the scope of cybercrime threats by exploiting information and communications technologies, including the darknet, to not only facilitate attacks but also create online markets for stolen data. Member States are taking steps to respond, including by increasing accessions to the Council of Europe Convention on Cybercrime. Using that Convention, countries from all regions (including both developing and developed countries) have strengthened national laws and improved their ability to cooperate with other countries in ways that also limit the ability of transnational criminal organizations to exploit their national information and communications technology infrastructure for criminal purposes.

403. The third challenge concerns limited national capacity and outdated national legal frameworks The United States faces challenges in working with partners to prosecute cybercrime where those countries have limited capacity and/or have not updated their domestic legal frameworks and investigative authorities to address cybercrime. While some countries rely on general criminal statutes, specific cybercrime statutes are best. Despite lacking an agreed definition of cybercrime, there is general agreement on culpable conduct that establishes a core list of offences. The international community has over a decade of experience across many different legal systems in drafting effective, modern and comprehensive cybercrime laws. Such laws can be drafted in a technology-neutral matter, avoiding the need for frequent amendments. The Council of Europe Convention on Cybercrime has been the main inspiration for other instruments and is a model for domestic laws for countries with various cultural and legal traditions – including some Member States that are not considering accession. The efforts of the United States, together with other countries, to prosecute cybercrime are more successful when working with a country using cyber-specific laws.

404. The United States also faces challenges in working with countries that have successfully adopted cybercrime-specific statutes, but that may either have limited capacity to implement their legal framework or may not have taken steps to do so in practice. In addition, the United States continues to face serious challenges in receiving assistance from some Member States to identify, apprehend and prosecute offenders in their jurisdictions and to authorize their authorities to cooperate internationally in cybercrime cases. For instance, there is an urgent need for specialized training in electronic evidence for criminal justice authorities. This is why the United States is a donor to the UNODC Global Programme on Cybercrime, as well as training programmes under the auspices of the Organization of American States, the Council of Europe, ASEAN and the African Economic Community. The United States recommends that Member States deepen their focus on such programmes, particularly for developing countries. Member States should prioritize both legislative reform assistance and capacity-building to ensure that new laws translate into action.

405. The fourth challenge concerns difficulties in obtaining electronic evidence. In the same way as other Member States, the United States faces challenges in receiving access to electronic evidence, which is becoming ubiquitous in law enforcement investigations, from foreign jurisdictions in the fight against cybercrime. Specifically, the United States faces challenges in receiving assistance from Member States that lack the legal authority or capacity to effectively respond to requests for electronic evidence.

406. Internally, the United States faces challenges in executing the thousands of requests from other jurisdictions for electronic evidence, often because those countries do not understand the United States requirements or provide insufficient information to meet United States legal standards. Insufficient mutual legal assistance requests require United States authorities to seek clarification and additional information from international partners, delaying the response to requests. Member States should work to overcome these gaps by empowering central and competent authorities with sufficient resources and training, consistent with their obligations

under instruments such as the Organized Crime Convention. Work is also under way at UNODC to provide new tools for central and competent authorities. The United States further recommends increased capacity-building for Member States on mutual legal assistance requirements and procedures, including training on drafting sufficient requests for electronic evidence.

407. Finally, to obtain electronic evidence, Member States are utilizing bilateral mutual legal assistance treaties, as well as multilateral conventions such as the Council of Europe Convention on Cybercrime and the Organized Crime Convention, as a legal basis for cooperation. Over 80 countries also actively participate in the Group of Seven 24/7 High-Tech Crime Network Points of Contact to facilitate data preservation and other requests. The United States recommend that Member States consider joining and utilizing such treaties and networks in the fight against cybercrime.

Venezuela (Bolivarian Republic of)

408. The Government of the Bolivarian Republic of Venezuela acknowledged the growing use of information and communications technologies and that the role of the international community in the use of these technologies could contribute to the achievement of internationally agreed development goals, including those contained in the 2030 Agenda for Sustainable Development, and to addressing new challenges.

409. The Bolivarian Republic of Venezuela underlined the importance of removing barriers to reducing digital gaps, particularly those that hindered the full achievement of the economic, social and cultural development of countries and the well-being of their populations, particularly in developing countries. It stressed that the use of information and communications technologies, including social networks, that violated international law and were detrimental to the interests of Member States, should be terminated.

410. The Bolivarian Republic of Venezuela encouraged the joint work of the international community to ensure access to the information society and also encouraged respect for gender equality and the empowerment of women, cultural identity, cultural, ethnic and linguistic diversity, traditions and religions and ethical values.

411. The Bolivarian Republic of Venezuela reported that it aimed to achieve the responsible use and treatment of information by the media, in accordance with codes of conduct and professional ethics. The media in all its forms has an important role in the information society and information and communications technologies should play a supporting role in that regard. The Bolivarian Republic of Venezuela reaffirmed the need to reduce the international imbalances that affected the media, especially with regard to infrastructure, technical resources and the development of human skills.

412. For the Bolivarian Republic of Venezuela, the use of the media as a tool for hostile propaganda against developing countries with the aim of undermining their Governments was a matter of concern. In that regard, the Bolivarian Republic of Venezuela highlighted the need to promote alternative means of communication and sources of communication that were free, pluralistic and responsible and that reflected the realities and interests of the countries and peoples of the developing world.

413. In this sense, and aware that international criminal law instruments are currently insufficient to counter information and communications technology-related crimes, the Bolivarian Republic of Venezuela considered it necessary to create a United Nations convention on cooperation in that area that was approved and based on the consensus of the international community, in which all Member States were encouraged to build a responsible information society and assist in taking measures to avoid and refrain from any unilateral measure not in accordance with international law and the Charter of the United Nations and that prevented the full economic and

social development of the population of the affected countries and hindered their welfare.

414. For the Bolivarian Republic of Venezuela, this concern for the potential use of information and communications technologies in international conflicts, covert and illegal operations and attacks on third countries by individuals, organizations and States through the use of computer systems from other nations, requires that measures be taken within the framework of United Nations to achieve progress in the realization of a document that helps regulate the use and cooperation in this area.

415. In view of the concern generated by the expressed capacity of some Governments to respond to such attacks with conventional weapons, the Bolivarian Republic of Venezuela reiterated that the most effective way to prevent and address new threats was through joint cooperation among all States, thus avoiding the conversion of cyberspace into a theatre of military operations. The Bolivarian Republic of Venezuela considered it a priority to promote dialogue and ongoing discussion among Member States in order to share good practices and national or regional experiences, paying special attention to developing countries. Likewise, the Bolivarian Republic of Venezuela expressed support for the proposal to create an intergovernmental working group, under the auspices of the United Nations to search for solutions and resolution of differences, based on the equality of States.

416. The Bolivarian Republic of Venezuela also recognized that the illicit use of information and communications technologies could have a detrimental impact on the infrastructure, national security and economic development of a Member State, and therefore emphasized the need to increase international efforts to address that problem.