United Nations system CEB/2013/2

Chief Executives Board for Coordination

13 January 2014

Original: English

Second regular session of 2013
New York, 25 November 2013

Summary of conclusions

I. Introduction

1. The second regular session of the United Nations System Chief Executives Board for Coordination (CEB) of 2013, chaired by the Secretary-General, was held at United Nations Headquarters in New York in the morning of 25 November 2013. In the afternoon, following the conclusion of the session, the Board held its second review of implementation of the Millennium Development Goals at the country level.

2. A retreat was held on 26 November at which executive heads had an exchange of views on the post-2015 process, followed by a private meeting of CEB, during which it considered political, economic, social and human rights issues on the United Nations agenda.

3. The present report covers the outcome of the second regular session of CEB of 2013.

4. On behalf of CEB, the Secretary-General welcomed new members: Li Yong, Director-General of the United Nations Industrial Development Organization (UNIDO); Mukhisa Kituyi, Secretary-General of the United Nations Conference on Trade and Development (UNCTAD); Phumzile Mlambo-Nguka, Executive Director of the United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women); and the new Secretary of CEB, Kim Won-soo.

5. The Board adopted the following agenda for its second regular session of 2013:

1. Adoption of the agenda.
2. Reports of CEB high-level committees:
   (a) High-level Committee on Programmes;
   (b) High-level Committee on Management;
   (c) United Nations Development Group.

14-20568 (E) 230114

3. Issues of system-wide concern: cybersecurity/cybercrime and policies on information.

4. Other matters.

II. Reports of CEB high-level committees

A. High-level Committee on Programmes

6. Achim Steiner, Chair of the High-level Committee on Programmes, introduced the report of the Committee on its twenty-sixth session, held at the headquarters of the Office of the United Nations High Commissioner for Human Rights (OHCHR) in Geneva on 17 and 18 October 2013. The session covered a number of issues of significance for system-wide coherence efforts. He expressed his gratitude to the United Nations High Commissioner for Human Rights, Navi Pillay, for hosting the Committee. The setting was ideal for its first in-depth consideration of the centrality of human rights in the work of the United Nations system. The fact that the outcome document of the United Nations Conference on Sustainable Development issued a strong call for human rights-based policy coherence in the post-2015 agenda showed the clear progress made in recent years in mainstreaming human rights into development work, and in linking human rights with peace and security and the rule of law.

7. The Chair of the Committee noted, however, that a number of challenges remained and, along with them, the need to establish stronger accountability mechanisms at all levels, in normative and operational work and through invigorated advocacy as United Nations system leaders. As such, the Committee stood behind the call by the Secretary-General to “renew our commitment to the peoples and purposes of the United Nations” and was prepared to support the implementation of the “Rights up front” action plan if so requested by CEB.

8. Mr. Steiner recalled that the session of the Committee had been held just days after the High-level Dialogue on International Migration and Development and the earlier launch of the publication prepared by the Committee on behalf of CEB, “International Migration and Development: Contributions and Recommendations of the International System”. He thanked the United Nations Population Fund (UNFPA), the Department of Economic and Social Affairs and the International Organization for Migration (IOM) for their leadership in the preparation of the contribution by the system to the high-level dialogue, which found good reflection in the declaration. He added that the critical stage of implementation was now upon us, including the appropriate inclusion of the issue in the post-2015 development agenda. The Committee had suggested that CEB might wish to request the Global Migration Group to formulate a synthesis of follow-up action to be taken by the United Nations system for review at its next session.

9. Through a working group led by the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU), the Committee had finalized for the endorsement of CEB a United Nations-wide framework on cybersecurity and cybercrime. The framework established principles for programme development activities related to cybercrime and cybersecurity, in support of Member States, and was accompanied by a compendium of relevant

United Nations system mandates. The Chair of the Committee noted the important linkage with the efforts of the Information and Communications Technology Network and the High-level Committee on Management on the matter.

10. Mr. Steiner briefly touched upon the other issues taken up by the High-level Committee on Programmes at its recent session. Members had agreed to work closely together to achieve system-wide coherence on drug policy and to support preparations for the special session of the General Assembly to be held in 2016. In follow-up to General Assembly resolution 67/220, the Committee also endorsed a number of recommendations related to system-wide support to the Office of the High Representative for the Least Developed Countries, Landlocked Countries and Small Island Developing States with regard to the implementation of the Programme of Action for the Least Developed Countries for the Decade 2011-2020. The Committee also took note of preparations for the CEB review of implementation of the Millennium Development Goals, and of briefings on the respective work of UN-Water and UN-Energy, including aspects related to the post-2015 development agenda.

11. Mr. Steiner pointed out that the Committee had met shortly before the United Nations Climate Change Conference, held in Warsaw in November 2013, and had considered both the preparations for the Conference, including the CEB high-level side event, and preparations for the Climate Summit 2014. The issue of climate change, along with that of a post-2015 development agenda, were twin pillars of a more sustainable world, as the Secretary-General had noted. The Committee, through its Working Group on Climate Change, was extending its full support to help ensure that emissions could be reduced without undermining development. He expected that work, which was being undertaken in full collaboration with the Climate Change Support Team of the Secretary-General, would accelerate over the next two years. Mr. Steiner also underscored the importance of sending a signal of unity within the United Nations system to Member States, which were themselves enjoined to pursue integrated approaches. This had been the focus of the CEB high-level side event at the United Nations Climate Change Conference, which the Chair of the Committee had been privileged to moderate, under the leadership of the Secretary-General, and with the participation of the Administrator of the United Nations Development Programme (UNDP) and the Secretary-General of the World Meteorological Organization, as well as of government and private sector representatives.

12. Indeed, the aim of the Committee continued to be to serve CEB in identifying and responding proactively to emerging policy and programmatic issues of concern to the entire United Nations system. For that reason, the Committee deepened its reflection of the salient issues related to the post-2015 development agenda on the basis of an issues paper that addressed two topics: the conceptual framework and how the United Nations system could be positioned in it; and rendering the United Nations system “fit for purpose” in the context of the new expectations and requirements that might arise from the post-2015 framework.

13. Mr. Steiner noted that, while it was in a transitional phase, the next 18 to 24 months would be critical for the United Nations system to assert its leadership in providing guidance and conceptual advice to the process, led by Member States, of crafting a future development agenda and in reaffirming the relevance and readiness of the United Nations system in supporting Member States in the implementation of

that agenda. He stressed the strong view expressed by all that CEB was essential to establishing the required shared system-wide commitment to policy coherence and appealed for a nexus approach that would bring together the various thematic and sector focuses of the United Nations system work. Indeed, this was doubly important given the multitude of ongoing intergovernmental and inter-agency processes under way. He concluded by noting that CEB would pursue a reflection at its retreat meeting on the constituent elements of a United Nations system that was fit for purpose for all people in the rapidly changing global environment, informed by a short discussion paper synthesized from consideration of the item by the Committee.

14. Finally, the Chair of the Committee paid special tribute to Elliott Harris, who had stepped down as Vice-Chair given his recent appointment as Director of the United Nations Environment Programme office in New York. He welcomed Gunilla Olsson, Director of United Nations and Multilateral Affairs of the United Nations Children's Fund (UNICEF), who would be joining the Committee as its Vice-Chair at its next session.

15. The Secretary-General thanked the Chair of the Committee for his briefing and announced plans for the Climate Summit, which would be held in New York on 23 September 2014, one day before the opening of the general debate of the General Assembly at its sixty-ninth session. He noted that the Summit presented a unique opportunity to leverage unprecedented financial, political and organizational capital. It was his intention that the Summit focus on solutions; to that end, leaders from Governments and all relevant sectors were invited to bring bold announcements and actions. The Summit had two primary goals: to raise political will for an ambitious global legal agreement by 2015; and to catalyse concrete action on all climate-related issues. The Summit would involve a plenary meeting for world leaders, as well as multi-stakeholder sessions that would bring together key actors from Governments, finance, business and civil society. Virtual platforms would be utilized to enhance the reach of the Summit beyond United Nations walls. The Secretary-General looked forward to the engagement of CEB members in this undertaking.

16. The United Nations High Commissioner for Human Rights, Ms. Pillay, commended Mr. Steiner for his admirable leadership of the Committee. She was pleased to have served as host for the Committee at its twenty-fifth session and stressed that Palais Wilson, the United Nations human rights house, was open to all CEB members. Indeed, human rights were being restored to the place envisioned for them in the Charter of the United Nations, that is, at the centre of all that the United Nations system did. Recent years and months had seen the adoption of an unprecedented number of policy developments in that field, which today were transforming the way the United Nations did business, from development, to economic and social affairs, to peacekeeping and humanitarian assistance, and placing new expectations and demands on all CEB members at all levels, whether at Headquarters or in the field. She thanked colleagues for their dedication and trusted that she could continue to rely on their support.

17. Ms. Pillay also thanked the Secretary-General for his leadership, as demonstrated through the International Recovery Platform follow-up process, by placing human rights at the centre of crisis situations. She was pleased to see that CEB was duly following up with its previous decisions by including human rights as

a regular item on the agenda of the Committee and maintaining a briefing during the private session. She encouraged CEB to endorse the statement by the Secretary-General on “renewing our commitment to the peoples and purposes of the United Nations”.

Briefing by Michel Jarraud, Chair of UN-Water

18. Michel Jarraud, Chair of UN-Water, briefed the Board on the outcome of the nineteenth meeting of the body, which was held in Stockholm in August 2013, as well as on recent developments. UN-Water was deeply engaged in strategic work related to the post-2015 development agenda. Thanking UNDP for its leadership of this work, he noted that UN-Water technical advice on a possible water goal would be launched on 29 January 2014 in New York at an event for Member States and other stakeholders. He invited colleagues, if available, to attend.

19. He noted that the campaign on the 2013 International Year of Water Cooperation would shortly be concluded and that the closing ceremony would be hosted by the Government of Mexico in Mexico City. Mr. Jarraud warmly thanked the United Nations Educational, Scientific and Cultural Organization (UNESCO), along with the Economic Commission for Europe and the Department of Economic and Social Affairs, for the coordination on behalf of UN-Water of the very successful campaign, which had seen a number of high-level events around the world, including in The Hague, New York, Dushanbe and Nairobi.

20. Looking ahead, the 2014 World Water Day campaign would focus on the theme “water and energy”. The United Nations University and UNIDO would lead efforts on behalf of UN-Water, in close collaboration with UN-Energy. Starting in 2014, the UN-Water flagship publication, the World Water Development Report, would be published on an annual basis and with a greatly improved format. The report would be released on World Water Day, with “water and energy” as its theme.

21. Mr. Jarraud noted that 19 November was World Toilet Day. Member States had asked UN-Water to support this campaign, which was an excellent opportunity to redouble efforts to fulfil the sanitation agenda towards 2015 and beyond. Finally, he thanked the Department of Economic and Social Affairs and the United Nations Office for Project Services (UNOPS) for the secretariat and administrative support arrangements provided for UN-Water.

22. The Director-General of UNESCO, Irina Bokova, thanked Mr. Jarraud for his leadership of UN-Water, underscoring that the 2013 International Year of Water cooperation had been very successful. UNESCO had organized five regional high-level events that had taken place around the world involving multiple stakeholders, including the private sector. She noted a growing momentum in the area of water diplomacy and highlighted the important efforts under way in water and sanitation. With regard to the World Water Development Report, there was a small issue with respect to a publications policy that needed to be addressed. She very much looked forward to an important contribution of this sector to the post-2015 development agenda, emphasizing that water security issues would become increasingly important in this context.

Briefing by Kandeh Yumkella, Chair of UN-Energy

23. The Special Representative of the Secretary-General and Chief Executive Officer of the Sustainable Energy for All initiative, and Chair of UN-Energy, Kandeh Yumkella, briefed the Board on recent activities undertaken by UN-Energy and provided an update in Sustainable Energy for All and other energy-related initiatives. Noting that energy was inextricably linked to many of the current global challenges, including poverty, food security, water, health, education, economic growth, youth and women's empowerment and climate change, he emphasized that energy must be fully integrated into the post-2015 development agenda. Momentum was already building among Member States and other stakeholders in support of a global goal on energy as part of the future sustainable development goals. Underpinned by a set of targets, such a goal would signify that energy was a nexus issue and an enabler of sustainable development.

24. He continued by stating that the General Assembly had declared 2014-2024 to be the United Nations Decade on Sustainable Energy for All. The launch of the Decade provided the United Nations system and other partners with significant opportunities to advance the energy agenda towards further actions for greater sustainability and accessibility. Recalling that more than 70 countries had already partnered with the initiative, he informed CEB that the Sustainable Energy for All initiative had been making progress in catalysing actions and commitments to sustainable energy by a range of actors, including Governments, the United Nations system, multilateral development banks, the private sector and civil society.

25. Turning to the work of UN-Energy, he noted that the inter-agency mechanism had strengthened its work in support of ongoing processes related to energy, including the Sustainable Energy for All initiative, the deliberations of the Open Working Group on Sustainable Development Goals, the follow-up to the United Nations Conference on Sustainable Development and the preparations for the United Nations Decade on Sustainable Energy for All. For example, UN-Energy was working on a detailed report aimed at aligning and coordinating, in a more coherent manner, the different efforts undertaken by the United Nations system to support the Decade and other related processes and initiatives. In concluding, he thanked CEB members for their support and invited them to consider additional measures to reinforce the work of UN-Energy.

26. **CEB endorsed the report of the High-level Committee on Programmes on its twenty-sixth session (CEB/2013/6), as well as the Secretary-General's statement, entitled "Renewing our commitment to the peoples and purposes of the United Nations" (see annex I).**

27. **The Board thanked Messrs. Jarraud and Yumkella for their briefings and leadership, respectively, of UN-Water and UN-Energy.**

B. High-level Committee on Management

28. The Chair of the High-level Committee on Management, Francis Gurry, introduced the report of the Committee on its twenty-sixth session, held on 10 and 11 October at the United Nations Office at Geneva.

29. The twenty-sixth session of the Committee was primarily focused on how the Committee is translating into action the strategic priorities included in its strategic

plan for 2013-2016, which the Committee adopted and the Board endorsed at their first regular sessions in 2013.

30. The Chair of the Committee underlined that the new strategic plan embodies the vision of the Secretary-General on management reform in the United Nations system and is designed to offer a substantial support to the Secretary-General in delivering on his Five-Year Action Agenda.

31. For the first time, through the quadrennial comprehensive policy review of operational activities for development of the United Nations system, CEB member organizations have a strong and comprehensive intergovernmental mandate to use the Committee as an instrument to redesign and operationalize an administration function more adaptive and agile in delivering programmatic mandates.

32. The strategic plan revolves around specific or broader requests from the quadrennial comprehensive policy review, as the Committee offers a useful platform for member organizations to devise and implement the appropriate response to the operational mandates of the quadrennial comprehensive policy review that require policy coordination and the engagement of headquarters. The Committee aims to report back to CEB in line with the time frames identified in the quadrennial comprehensive policy review, for the Secretary-General to be able to meet his reporting requirements as identified in General Assembly resolution 67/226 on the quadrennial comprehensive policy review of operational activities for development of the United Nations system.

33. Through continuing coordination with the United Nations Development Group, the Committee will also ensure consistency of action with country-level operational activities. In that regard, the Committee is actively engaged in the monitoring framework discussions led by the Department of Economic and Social Affairs.

34. The Chair of the Committee focused his briefing on the work of the Committee in the area of human resources management. Among the current top priorities for the Committee, one key priority is to engage in a dialogue with the International Civil Service Commission (ICSC) in the context of its review of the conditions of service for United Nations system staff, with the aim of developing a proposal for a competitive and simplified compensation package that enables organizations to attract and retain staff of the highest calibre and reduces transaction costs.

35. The Vice-Chair of the Committee, Jan Beagle of the Joint United Nations Programme on HIV/AIDS (UNAIDS), is leading that work on behalf of the Committee, through a high-level steering group composed of selected Committee representatives who will provide strategic guidance and support throughout the exercise. The review will comprise the following three areas: remuneration structure; competitiveness and sustainability; and performance recognition and other relevant human resources issues.

36. The Chair introduced the draft CEB statement that was before the Board for consideration and approval. He recalled the main principles and the outcomes expected from the review, as reflected in the statement, and underlined how important it is for organizations to stay engaged in the process and maintain the initiative in order to ensure that their needs and requirements are properly addressed within the new United Nations common system that will be designed and put in place by way of the review.

37. The Chair also stressed that organizations must be strategic and look above the current contingent circumstances and constraints, towards an outcome that must respond to the essential objectives of having the right instruments to operate effectively, not losing the competitive advantage and remaining relevant.

38. Finally, the Chair noted that the draft statement placed an emphasis on the fact that the ICSC review should be based on common principles and implemented with the flexibility needed to meet different organizational needs. It should promote innovation, transparency and cost-effectiveness and reduce transaction costs through simplification.

39. Among the other top priorities of its strategic plan, the Chair of the Committee informed the Board that the Committee had chosen to focus on the development of an organizational environment that recognizes good performance, strengthens linkages to career development and sanctions poor performance.

40. Some member organizations have made considerable advancements in that area and all are actively engaging in initiatives towards that end. UNOPS, the International Fund for Agricultural Development and, more recently, the World Intellectual Property Organization are now at an advanced stage in the piloting of rewards, recognition and sanctions policies. At the same time, other organizations, like UNFPA, are reporting on their successful implementation of performance appraisal systems that allow for a more effective and legally solid recognition of superior and inferior performance.

41. The Chair reported that, at its last meeting, in October 2013, the Committee had received presentations on such recent experiences, which many are now looking at for inspiration and as a basis for modelling their individual initiatives to develop schemes to manage performance and reward achievements.

42. Finally, the Chair reminded the Board that the General Assembly was about to start its deliberations on the ICSC recommendation to increase the mandatory age of separation to 65 for current staff members, as of 1 January 2016.

43. He recalled that organizations had expressed strong concerns regarding that proposal, as many of them are at different stages in organizational and workforce realignment efforts, including for gender balance, and the current arrangements for the mandatory age of retirement are facilitating workforce planning in those situations. At the same time, convincing arguments and solid evidence of the benefits that the change would produce have yet to be provided.

44. The Chair concluded, recalling the recommendation by the Committee at its October meeting, that executive heads should consult with Member States to ensure that they are provided with the necessary flexibility to phase-in mandatory separation at 65 for existing staff, in a way that would enable smooth organizational and workforce planning, according to individual organizational needs.

45. In the ensuing discussion, Jose Graziano da Silva stressed the vital need for containment of staff costs, which represent 75 per cent of the regular programme of the Food and Agriculture Organization of the United Nations (FAO). He also emphasized the need for more flexibility and discretion for executive heads to tailor the compensation package for specific purposes, especially to encourage staff mobility, and to maintain staff in the most difficult field duty stations. Finally, he

expressed the wish that the current compensation package review would lead to a system that is extensively simplified and less expensive to administer.

46. The Secretary-General thanked the Chair of the Committee for his briefing, noted that the concerns expressed by the Director-General of FAO were fully shared and acknowledged the letter received from the Geneva group, noting the words of appreciation by the Member States towards the work of the Committee in promoting a more joined-up approach to change across the United Nations system and in finding efficiency savings while improving delivery.

47. **The Board took note of progress and endorsed the conclusions of the High-level Committee on Management at its twenty-sixth session (CEB/2013/5), and adopted the CEB statement on the ICSC review of the common system compensation package (see annex II).**

C. United Nations Development Group

48. The Chair of the United Nations Development Group, Helen Clark, introduced the reports of the meetings of the Group, held on 9 May and 19 September 2013.

49. The Chair of the Group highlighted that General Assembly resolution 67/226 had been a major impetus for reform and that the Group had been placing the highest priority in 2013 on ensuring that the quadrennial comprehensive policy review was coherently implemented across the United Nations development system, with a firm focus on high-impact priority areas. The Group had agreed on the first ever common action plan for the quadrennial comprehensive policy review and United Nations agencies had taken significant strides to internalize the quadrennial comprehensive policy review mandates into their strategic plans. The Chair of the Group highlighted that the Department of Economic and Social Affairs and the Group had developed a coherent monitoring and reporting framework for the quadrennial comprehensive policy review that was robust, evidence-based and cost-effective, while imposing a minimum reporting burden on Governments and the United Nations system.

50. The Chair of the Group noted that the development of standard operating procedures for “Delivering as one” countries had been a major breakthrough in 2013. “Delivering as one” had already become the working modality of choice in 35 countries. The Group expected demand to rise for “Delivering as one” as United Nations country teams embarked on developing new United Nations Development Assistance Frameworks in 100 countries over the next three years. The standard operating procedures intended to shift the emphasis from entities of the United Nations system conducting planning together, to delivering measurable results and robust monitoring, evaluation and reporting together. To ensure that the standard operating procedures had their intended impact on coherence, effectiveness and simplification at the country level, the Group would adopt before the end of the year a plan of action that outlines priority actions to be addressed at Headquarters and by United Nations governing bodies.

51. The Chair of the Group emphasized the need for strong political commitment from CEB members to the implementation of system-wide cost-sharing of the resident coordinator system by all member organizations of the Group, beginning in 2014. Even though the Group cost-sharing agreement was described as not a “lavish

scheme and barely meets the basic requirements of the system", the funding gap still amounted to $8.3 million in 2014 and $12.5 million in 2015. While nine organizations had committed to contributing their full shares in 2014, nine other organizations had only committed reduced amounts or no contributions at all. The Chair of the Group stressed that such lack of commitment would seriously jeopardize the ability of the United Nations development system to coordinate effectively at the country level. Noting that the Group was committed to begin implementing the cost-sharing agreement to the extent possible in 2014, she called upon member organizations of the Group, including the United Nations Secretariat, to redouble their efforts to fund the agreed formula and contribute their full shares, including pro forma cost adjustments, before the end of the year.

52. Anthony Lake, Executive Director of UNICEF, supported Ms. Clark's efforts but expressed his concern at the calls from Member States for more coordination and effectiveness but their lack of financial support for achieving such objectives, putting the Resident Coordination system at risk. Babatunde Ostimehin, Executive Director of UNFPA, also thanked Ms. Clark for her leadership.

53. Taleb Rifai and Michel Jarraud, Secretaries-General of the World Tourism Agency (UNWTO) and the World Meteorological Organization (WMO) respectively, while reiterating their interest and expectation to remain part of the system, expressed strong concern at the cost-sharing formula being put forward and called for more flexibility to address the special circumstances of smaller agencies that do not require the same kind of services, have very limited country-level engagements and have to function with much smaller budgets.

54. Ms. Clark addressed these concerns, reiterating that such considerations had been taken fully into account in the present formula, which not only made allowances for separate base fees for small and large agencies, but also took into account budget sizes for staff and for development activities, as well as the scale of involvement of each participating organization in the programmes of the United Nations Development Assistance Framework. She added that humanitarian agencies were also charged differently, as their coordination costs were handled separately. Finally, she mentioned that the current funding being sought was some $11 million less than when the negotiation started in 2011.

55. The Secretary-General requested the Chair of the United Nations Development Group to consult further with UNWTO and WMO on the strong concerns of those agencies regarding the cost-sharing scheme.

56. **With that understanding, the Board took note of progress and endorsed the reports of the United Nations Development Group.**

III. Issues of system-wide concern: cybersecurity/cybercrime and policies on information

57. In introducing the item, the Secretary-General noted the need for a substantive discussion on this very sensitive issue, which has been highly visible in the press in recent months. He noted that there exists a general awareness of how the information society has revolutionized many aspects of global society, including sensitivity to the risks of insecurity of the information age, indicating that computer viruses, theft of intellectual property and the use of technology for criminal

behaviour are nothing new. However, a growing awareness of the loss of privacy, coupled with a growing awakening to the risks to global security, has fed a growing urgency to take action to protect the work of the United Nations system and the populations that are served. Recent events have revealed the scale of private information that is collected and analysed by various actors and have spurred both the public and private sectors to act. The increasing attention to the issue was highlighted during the general debate of the General Assembly at its sixty-eighth session, when the first speaker, the President of Brazil, dedicated significant time to the issue.

58. It is well known that cyberattacks have the potential to destabilize on a global scale and must be a matter of global concern. The Secretary-General noted that CEB has discussed the item previously and the High-level Committees have taken action. Now that the system has a framework to support Member States, as presented and endorsed by the High-level Committee on Programmes, the challenge is to follow through in integrating its principles in the work of all three Committees. Progress in the High-level Committee on Management is equally important, as enhancing the capacity of agencies to resist cyberthreats must remain a priority. Furthermore, the United Nations system must also strengthen its collective ability to guide Member States towards a more global approach to the issue, especially as many intergovernmental processes remain narrow in scope. Clearly, the issue requires engagement by Member States on all fronts. Information technology has transformed our lives and helped advance the ability of the United Nations system to bring peace, prosperity and dignity to the world. The challenge now is to explore how the agencies of the United Nations family can protect those gains and identify the steps needed to create a more secure cyberenvironment.

59. Thanking the Secretary-General of the United Nations, the Secretary-General of ITU, Hamadoun Touré, noted that bringing the issue to CEB marked the beginning of a new era, where the United Nations system begins to develop a holistic and coordinated approach to assist Member States in regaining trust in the use of information and communications technology (ICT). The many challenges to bridging the digital divide that remain are technical issues that can be solved over time, whereas what the world faces today is not only a challenge, but a threat to the confidence in the ability to securely communicate. Furthermore, the effects of recent global events, and the reactions of Member States, have demonstrated that the United Nations system must move quickly to address the issue of cybersecurity as Member States are already taking steps at the national, regional and international levels.

60. Mr. Touré noted that, as the world has become massively more connected, with an increasing proportion of human activity occurring online, a secure information environment has become fundamental to the broad range of issues and principles that concern the United Nations system, from the rule of law, peace and security, development, governance, human rights and disaster risk reduction, to preparedness and mitigation. He stressed that all of those principles are at stake unless the United Nations system quickly begins to address “virtual world” issues, and cited a recent remark by a Member State that “a single cyberattack against core telecommunication infrastructure could cause more global disruption than a single physical attack”.

61. Noting with appreciation the commitment of the Secretary-General to a multidisciplinary approach to cybersecurity and cybercrime as the way forward

under the auspices of CEB, Mr. Touré outlined a series of actions that the United Nations system could take in support of the issue, including:

- Conveying a consistent message from the United Nations system to help parties focus on priority areas that enhance confidence in cyberspace
- Promoting joint programming, harmonization and cooperation in cyberspace-related activities of the organizations of the system
- Supporting high-level dialogues that address the challenge of balancing security, human rights and economic development with the rule of law and good governance
- Supporting preparations to include cybersecurity matters into the post-2015 development agenda
- Implementing the principles contained in the United Nations-wide cybersecurity and cybercrime framework
- Developing and sustaining inter-agency capacity to deploy secure, reliable and efficient information systems

62. Mr. Touré expressed satisfaction with the excellent work done by the High-level Committee on Management and the High-level Committee on Programmes, but noted the need for an enhanced United Nations-wide holistic and coordinated approach, especially given the diverse range of inter-agency mechanisms currently engaged in various aspects of the issue, including not only the High-level Committee on Management and the High-level Committee on Programmes, but also the task force of the High-level Committee on Programmes on cybersecurity and cybercrime, the United Nations Group on the Information Society, the United Nations Development Group, the Information and Communications Technology Network and its subgroups. To help move towards a more coordinated approach and to address the six action items mentioned, Mr. Touré expressed willingness to dedicate resources to the effort and hoped that other and larger agencies would do the same.

63. The representative from UNODC, Aldo Demoz-Lale, noted that, when it came to cybercrime, many intergovernmental bodies had examined the issue, including the First, Second and Third Committees of the General Assembly and the Economic and Social Council, as well as the Security Council, in a 2010 statement by the President in which he acknowledged the growing global threat of cybercrime. Echoing the remarks of ITU, UNODC noted that, in today's hyperconnected world, where currently one third of the world has Internet access and it is estimated that, by 2017, as much as two thirds of the world will have mobile broadband access, it is difficult to imagine any crime that does not involve electronic evidence linked with Internet connectivity. Cybercriminality is advancing much faster than Governments can keep up with and, as a result, international criminal groups are stronger than ever and the impact of their activities is seen everywhere. Noting that cybercrime describes a wide range of offences, including offences against computer data and systems such as hacking, computer-related forgery and fraud such as phishing, content offences such as disseminating child pornography, copyright offences such as the dissemination of pirated content and other offences such as incitement to terrorism and computer-related terrorist financing, the focus of concern is currently on an upsurge in technology-assisted illicit drug trafficking.

64. Regarding the framework developed by the High-level Committee on Programmes on cybersecurity and cybercrime, UNODC expressed satisfaction with the outcome, indicating that the United Nations system had taken a strong first step in addressing the matter in a coordinated and comprehensive manner. In addition to the framework document, the compendium, which includes mandates of the United Nations and various frameworks, provides United Nations entities and Member States with a major tool in their fight against cybercrime and demonstrates the broad range of United Nations agencies that are involved in the delivery of technical assistance and support in this area. In closing, UNODC stressed that it is of utmost importance that the United Nations system take a coordinated and consistent approach when supporting Member States in the area of cybersecurity and cybercrime.

65. The Director-General of UNESCO, Irina Bokova, indicated that UNESCO had not been listed in the compendium of United Nations mandates on cybersecurity and cybercrime contained in the report by the High-level Committee on Programmes on the draft United Nations-wide framework on the subject, when in fact UNESCO has a clear mandate on action line 10 of the World Summit on the Information Society. She noted that her organization had been affected by the recent events regarding cybersecurity and informed the Board that the recently concluded thirty-seventh session of its General Conference included a draft resolution entitled “Internet-related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society”. In the resolution finally adopted by consensus after an intensive debate, the General Conference requested the Director-General to prepare a comprehensive study of the Internet-related issues within the mandate of UNESCO, including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society, containing possible options for future actions through convening an inclusive multi-stakeholder process, which includes Governments, the private sector, international organizations and the technical community. The text of the resolution (37 C/61), which she quoted, will be shared with CEB members. Ms. Bokova noted that it was apparent that Member States were entering a new phase of discussion regarding the issue of privacy and security in the information age. She emphasized that this is a debate that is profoundly driven by Member States and that ownership by Member States of the process will be critical.

66. In concluding her remarks, Ms. Bokova noted that UNESCO had been entrusted by the outcome process of the World Summit on the Information Society with the responsibility of coordinating activities related to action line 10, on ethics in the information society. She noted that, as part of that work, UNESCO had produced studies, including a 2012 report on the ethical dimensions of the information society. She underlined the good cooperation UNESCO enjoyed with ITU in the framework of the World Summit and the Broadband Commission for Digital Development.

67. Mukhisa Kituyi, Secretary-General of UNCTAD, began his remarks by thanking the Secretary-General for his efforts in bringing system-wide attention in a holistic way to the challenges of cybersecurity and cybercrime, especially as the membership is looking increasingly to the United Nations to offer solutions. Mr. Kituyi expressed full endorsement of the United Nations cybercrime and cybersecurity programme policy framework currently led by ITU, UNDP and UNODC. He stressed that one of the greatest challenges for the United Nations system is

reducing duplication of microsecurity environments within agencies and looking at broader holistic challenges to the integrity of system-wide communication systems.

68. Turning to issues of development, Mr. Kituyi noted the importance of information technology as a tool for development, indicating that, in some areas of the world, mobile money, for example, holds enormous potential for reaching the unbanked and enhancing financial inclusion. Today, e-commerce is one of the greatest drivers of new forms of wealth around the world and that phenomenon could yield much more in the recovery of the global economy if the integrity and privacy of the boundaries surrounding the electronic movement of services were enhanced. For developing countries, he noted two levels of challenges: the development of regulatory legislation and dispute resolution mechanisms. Agencies are working to support many countries in developing national legislative frameworks, but even more important are the efforts of the regional commissions in supporting the regional harmonization of privacy and data protection laws.

69. Beyond the development of laws lies the need for enforcement. There appears to be a lack of clarity as to who is responsible for training the courts, prosecutors and the police on enforcing emerging regulations on cybercrimes. As many developed economies are insisting on establishing domestic legislation on data protection as a precondition for trade, developing economies may find it difficult to respond. As a result, they could experience constraints on market access.

70. He suggested that there would be further challenges due to the emerging phenomenon of cloud computing, which could have profound effects on privacy unless the necessary regulatory frameworks are set up. Individuals who perform private transactions in the cloud have cybersecurity concerns as it becomes increasingly unclear which territory and which regime of laws apply.

71. In concluding, Mr. Kituyi suggested that there is a growing need to discuss within the United Nations system the mechanisms available to address cybercrime. He noted the similarity between cybercrime and climate change, where urgent efforts are needed to mitigate the worst effects. He called for a continued discussion within the United Nations system on a range of questions, including ways that the United Nations system can work to: strengthen the integrity of e-transactions; create shared access to transaction benefits of the technology for countries with limited capacity on e-regulation; provide leadership internationally in line with the outcomes of the World Summit on the Information Society and the follow-up work by the United Nations Group on the Information Society; and provide leadership in an internationally responsible way to mitigate threats to cybersecurity, including the protection of intellectual property rights and business information. Those are the areas where the United Nations system could provide leadership and focus its activities.

72. In her remarks, the Administrator of UNDP, Helen Clark, concurred with other speakers that cybersecurity had become essential to the protection of individual rights and privacy, the protection of the security of transactions and the protection of the good functioning of government and business. She suggested that, while cybersecurity is a growing global concern, cyberspace in developing countries is even more vulnerable because of their lower capacity to respond to cyberthreats, placing them more at risk and therefore requiring enhanced support. Building on the work of ITU, UNODC, UNCTAD and UNESCO at the global normative level, United Nations country teams could develop two sets of actions on the ground,

starting with raising awareness among constituents. Many agencies already have considerable normative experience that could be applied, especially among the least developed countries, which require the most support.

73. Furthermore, actions that the United Nations system could take on the ground include developing enhanced capacity by providing support to Governments, citizens and private-sector actors, given that various stakeholders have potentially divergent interests. While there is an obvious emphasis on security and cybercrime, a balance should be sought to support privacy, avoid illegal surveillance and limit military involvement in the area strictly to indispensable and clearly defined national security needs.

74. Ms. Clark informed the Board that a group of Governments and other actors, including Ghana, Malaysia, the Republic of Korea, the United Kingdom of Great Britain and Northern Ireland and the European Community, along with Microsoft and Oxford University, United Kingdom, have, together with UNDP, initiated policy discussions aimed at supporting programme countries in establishing multi-stakeholder alliances, including intergovernmental cooperation, and capacity development initiatives through the technical assistance of the United Nations system.

75. To move forward in this area, Ms. Clark suggested that, within the 70 countries of the United Nations Development Assistance Framework over the next two years, resident coordinators could raise with Governments the opportunity of including such issues as a feature of the next United Nations Development Assistance Framework. Furthermore, she expressed reluctance to include cybersecurity as an additional issue in the post-2015 development agenda, given the already substantial list of areas already under consideration, but indicated that in the context of the protection of vital infrastructure, cybersecurity should be something that merits further consideration. She concluded her remarks by reiterating the importance of protecting each of our agencies, mentioning that UNDP has been a target of cyberthreats in the past, that it has taken steps to mitigate those threats and that it fully supports inter-agency activities to strengthen internal capacity in the area.

76. After thanking ITU, UNODC, UNESCO, UNCTAD and UNDP for their insightful comments, the Secretary-General opened the floor for general discussion. The Under-Secretary-General for Communications and Public Information, Peter Launsky-Tieffenthal, informed the Board that, after closely monitoring both traditional and social media on the issue, it became apparent that, unlike most other issues of worldwide importance, this is an ongoing global discussion with a high emotional content. Furthermore, from an analysis of the discourse, it appears that the public expects, and in some ways demands, an active role by United Nations agencies, stressing that national efforts would not be credible. From a purely communications point of view, he is of the view that it is absolutely necessary and important that the United Nations be shown to be taking the lead. The Chief Information Technology Officer, Atefeh Riazi, reiterated the importance of addressing the issue of cybersecurity and cybercrime, stressing the vulnerabilities of critical infrastructure in many countries, as more of these systems are linked together using the public Internet. She also noted that agencies are currently lacking in robust mechanisms to address cyberthreats to their own infrastructure and welcomed measures to reduce system-wide cybersecurity response fragmentation.

77. The representative of the regional commissions, Alicia Bárcena, the Executive Secretary of the Economic Commission for Latin America and the Caribbean

(ECLAC), informed the Board of a process that is ongoing at the regional level whereby, at the request of Member States, ECLAC is re-establishing a forum to discuss ICT. The forum has proved very useful to address, inter alia, issues of infrastructure, security and access to broadband. She stressed the need to ensure inclusion of the private sector in discussions concerning cybersecurity and noted that the forum, although led by Member States, includes service providers, broadband providers and infrastructure providers. She noted that, given the current events regarding surveillance, the region is considering relocating its existing data centres within the region.

78. During the discussion, many Board members highlighted the sensitivity and complexity of the issue, which includes elements as diverse as human rights, privacy and the impact on development. On the human rights dimension of the issue of cybersecurity and cybercrime, several participants emphasized that all measures to counter cyberinsecurity and cybercrime must be in conformity with international human rights standards, including freedom of expression, information, opinion, association, privacy rights, dissemination of hate speech, racism, child pornography, abuse and trafficking in persons, and underscored the notion that cybersecurity must not only include the security of assets and the cyberenvironment, but also of individual users. Participants also noted that, although women and children tend to be victims of cybercrime in many ways, the opportunities afforded to those groups through universal access to the Internet underscored the "double-edged" nature of the issue, and therefore the importance of ensuring a secure cyberenvironment so that such opportunities can be enjoyed by all.

79. The issue of privacy also garnered the attention of Board members, with participants stressing the need to find a way to ensure that people's rights to privacy and freedom of expression are not limited, not to mention criminalized, by the use of enforcement practices by States and that, while concerns about national security and criminal activity may justify the exception for using surveillance programmes, such measures must come with adequate safeguards to protect the right to privacy. It was further noted that vulnerable and excluded groups depend on United Nations entities for protection and that data about those groups, such as where they reside, must be protected.

80. Many participants stressed the need to consider the impact of cybersecurity on development and the role of a cybersecure environment while considering actions in the post-2015 development area. Some noted that ICT will be critical to achieving results in social and economic development and that a cyberinsecure environment will only inhibit growth.

81. Another issue that CEB members raised was the need to regard cybersecurity as a component of risk management, both in the context of support to Member States as well as during the development of internal policies on information. By taking the proper precautions, Governments, civil society and the private sector can all enjoy the benefits that the information technology revolution offers, but in a manner that reduces the risks inherent in the use of such technology. Similarly, agencies may benefit from a deeper analysis of the types of information held by our institutions that require protecting, especially as organizations respond to demands of transparency.

82. In concluding its discussion, the participants generally agreed that the information and communication revolution touched on many different aspects of the

work of United Nations agencies, including crime, the role of women, climate change and youth unemployment. Furthermore, they agreed that all of the issues were part of a new global landscape and that CEB could be utilized as a vehicle for further work on integration and working as one.

83. In his final remarks, the Secretary-General of ITU thanked all contributors to the discussion. He noted that the issue goes deep into the heart of the mandate of the United Nations to protect peace and security, as there is currently a very real risk of cyberwar. The technology now allows for non-State actors to initiate those kinds of actions and there is a need for the United Nations to take the lead in working towards a safe and secure cyberspace.

84. In summarizing the discussion, the Secretary-General thanked all members for an interesting, thought-provoking and enlightening discussion. He noted that Member States were very engaged in the discussion. Technology, he noted, is in the hands of everyone, for both good and evil, but in today's world it functions as a cross-cutting tool that the world cannot do without.

85. The Board endorsed the United Nations-wide framework on cybersecurity and cybercrime (see annex III) and welcomed the initiative by the High-level Committee on Management to develop enhanced system-wide capacity to address cybersecurity threats to United Nations agencies. As a result of the discussions, and rather than make any decisions at the level of CEB at the present time, the Secretary-General called for ITU, together with UNESCO, UNODC, UNDP and UNCTAD, and in close coordination with the High-level Committee on Management, the High-level Committee on Programmes and the United Nations Development Group, to develop a system-wide comprehensive and coherent strategy for addressing the issue, for discussion at the second regular session of 2014.

IV. Other matters

A. Third International Conference on Small Island Developing States

86. The Secretary-General, referring to the third International Conference on Small Island Developing States, to be held from 1 to 4 September 2014 in Apia, noted that a number of member organizations had proposed that a high-level CEB side event be organized.

87. In the light of the successful event held in Rio de Janeiro, Brazil, which had showcased the collective capacity of the United Nations system to advance integration and coherence of the economic, social and environmental dimensions of sustainable development, he sought the support of Board members in organizing the side event to demonstrate what the United Nations system, working together, could tangibly contribute to the sustainable development of small island developing States.

88. The Board endorsed the proposal by the Secretary-General to hold a high-level side event during the third International Conference on Small Island Developing States.

B. Dates and venues of future sessions

89. Further to earlier consultations, the Board confirmed the dates of Thursday, 8 and Friday, 9 May 2014 for its first regular session of 2014 and thanked the International Fund for Agricultural Development, which would host the session in Rome.

90. CEB members would be consulted in due course on the dates of its second regular session for 2014, to be held at United Nations Headquarters in New York.

91. Finally, the Board accepted Ms. Bokova's kind invitation to hold its first regular session for 2015 at UNESCO headquarters in Paris.

C. Tribute to departing members

92. The Secretary-General, on behalf of CEB, paid tribute to Filippo Grandi, outgoing Commissioner-General of the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), and to Jan Mattsson, outgoing Executive Director of UNOPS.

93. He thanked Mr. Grandi for his determination, commitment, energy and strong leadership of UNRWA during an immensely challenging time. Despite all of the challenges facing UNRWA over the past four years, in the Syrian Arab Republic, Gaza, the West Bank, Jordan and Lebanon, UNRWA had successfully carried out its mandate, serving over 5 million increasingly vulnerable Palestinian refugees. He thanked him for all those efforts and his work to modernize and equip UNRWA for the challenges ahead.

94. Mr. Mattsson had served as Executive Director of UNOPS since mid-2006 and helped to show how reform and innovation could transform the work of the United Nations. Under his leadership, UNOPS had developed world-class expertise in sustainable project management, procurement and infrastructure and made a real difference for peacebuilding, humanitarian and development operations, often in some of the most challenging environments.

Annex I

Statement by the Secretary-General of the United Nations

Renewing our commitment to the peoples and purposes of the United Nations

The United Nations Charter expresses the determination of "We the peoples" to "reaffirm faith in fundamental human rights" and to establish conditions under which justice and respect for international law can be maintained.

The General Assembly, the Security Council, the Human Rights Council and other United Nations bodies have further defined the responsibilities of Member States and the United Nations system, with a special emphasis on their role to prevent armed conflict and to protect people from atrocities and egregious crimes.

When people face such risks, they expect the United Nations to act, and the Organization's performance is rightly measured by this benchmark. Every day, in zones of conflict, humanitarian emergency and insecurity, as United Nations staff, we try to meet our responsibilities to protect people. Staff often show tremendous courage and commitment, as in Timor-Leste in 1999. They sometimes give their lives to United Nations service.

Despite our efforts, the Member States and the Secretariat, agencies, funds and programmes have not always succeeded in achieving these goals. The 1994 Rwandan genocide represents the most emblematic failure of United Nations and Member State action. This was followed by our collective failure to prevent atrocities in Srebrenica in 1995. In 2012, my Internal Review Panel assessed United Nations action in the final stages of armed conflict in Sri Lanka as a "systemic failure" — a characterization I accept on behalf of the United Nations system.

Over these past two decades, several million people have lost their lives in such crises, and tens of millions have been displaced. Only by meeting our Charter responsibilities can the United Nations and its Member States prevent horrendous human suffering. We can and must improve how we react to impending catastrophes. A coherent United Nations, exercising its moral and political responsibility and taking early civilian action, can have a transformational impact in preventing and ending gross violations of human rights and humanitarian law. By doing this, the United Nations can support national mid regional actors to meet their own responsibilities, ultimately supporting sovereignty and encouraging peaceful resolution of conflicts.

The recommendations of the Internal Review Panel and its follow-up will help us to better achieve these goals. Implementation begins with this statement, launching a series of steps that will strengthen United Nations action. The statement is being shared with all staff members, for whom it can serve as a guide and reminder in their daily work.

On behalf of the senior leadership and all staff, I solemnly renew the commitment of the United Nations Secretariat, funds and programmes to uphold the responsibilities assigned to us by the Charter, the Security Council and the General Assembly whenever there is a threat of serious and large-scale violations of international human rights and humanitarian law.

We will be vigilant in identifying emerging risks and will ensure that our actions are guided by more effective use of the information that is available to us from United Nations human rights and humanitarian mechanisms and other entities.

We will inform national authorities of violations and support them in taking essential early action.

We will bring violations to the attention of the appropriate United Nations organs and regional organizations when national authorities are unable or unwilling to respond.

We will work to help Member States reach agreement on early actions and play our role in implementing their decisions.

We will speak out publicly where violations are ongoing.

We will exercise due diligence in implementing all our mandates.

We will engage in discussions with Member States on ways they can pursue improvements towards fulfilling their own responsibilities.

Above all, we renew our commitment to "We the peoples" of the Charter of the United Nations.

As we look at the Syrian Arab Republic and other difficult situations going forward, this commitment will be fulfilled promptly and systematically, with compassion, integrity, impartiality and with courage by us all.

BAN Ki-moon
21 November 2013

Annex II

Statement on the review of the common system compensation package by the International Civil Service Commission

1. The continued development of the international civil service as an independent, neutral, highly skilled and engaged resource is a key condition for the United Nations system to be able to effectively meet the ever-changing requirements of the international community.

2. Member organizations of the United Nations System Chief Executives Board for Coordination (CEB) reiterate their strong commitment and expectation to engage in a constructive dialogue with the International Civil Service Commission in the context of its review of the conditions of service for United Nations system staff.

3. CEB member organizations reconfirm their support for the continued application of the Noblemaire principle as the fundamental principle governing the conditions of service of professional and higher categories staff in the common system, as recently reaffirmed by the General Assembly (see resolutions 66/235 A and 64/231).

4. Through the ICSC review, United Nations system organizations aim to develop a competitive and simplified compensation package that enables organizations to attract and retain staff of the highest calibre, in the context of strategic workforce planning.

5. The ICSC review should be based on common principles and implemented with the flexibility necessary to meet different organizational needs. It should promote innovation, transparency and cost-effectiveness, reduce transaction costs through simplification, and rely on objective evidence from systematic data gathering and monitoring on relevant trends.

6. The long-term ability of organizations to sustainably deliver the broad spectrum of programmatic activity, with correspondingly different business models, in the multitude of geographic locations where the United Nations system operates, must be the primary and overarching assessment criterion for the Review.

7. In the view of CEB member organizations, a future compensation system should be informed by the following principles:

(a) *Fit for purpose and competitiveness*: it must be designed to be internationally competitive, and to attract, retain and promote high performing staff, cater for the broad set of knowledge-intensive skills and profiles needed by the United Nations system organizations to deliver on their respective mandates, and be fit for purpose and adaptable to their different business models;

(b) *Cost-effectiveness*: it should ensure predictability of staff costs and take in due consideration the financial situation of the organizations participating in the common system;

(c) *Equity*: it must be transparent. It should take in due consideration the expatriate nature and family status of internationally-recruited staff, who are part of a global mobile workforce and serve outside their home country for — most or the whole of — the duration of their tenure with the organizations;

(d) *Simplification*: it must be simple to understand for staff, organizations and Member States alike. It should also be easy to administer, thus resulting in the reduction of transactional costs;

(e) *Diversity*: it should preserve and promote the international nature of the organizations and their membership, ensuring the desired diversity among staff with regard to gender, geographic representation, age and other relevant criteria;

(f) *Motivating staff and rewarding performance*: it should provide for adequate recognition of performance;

(g) *Hazardous and hardship duty stations*: it should provide appropriate incentives for service in hardship and high-risk duty stations;

(h) *Mobility*: it should encourage geographical, inter-organizational and functional mobility, as appropriate to the mandates and business models of the individual organizations;

8. The ICSC review also presents an opportunity to renew the commitment of organizations to a cohesive and strong United Nations common system. In this spirit, CEB member organizations consider the following to be critical success factors:

(a) The review should be conducted in an open, evidence-based and consultative manner, allowing each organization of the common system to adequately contribute its requirements, expertise and knowledge to the discussion;

(b) The implementation of the new package and a communication strategy with the staff would need to be planned and agreed in a consensual manner with the organizations, in order to minimize any change-management-related risks;

(c) Acquired rights would have to be duly taken into consideration, including, where applicable, in transitional measures for current staff members;

(d) Organizational flexibility should be provided for in the implementation of the outcome of the review.

9. CEB member organizations look forward to a review whose scope remains limited to subjects directly related to compensation elements under the purview of ICSC.

Annex III

United Nations-wide framework on cybersecurity and cybercrime

Introduction

1. The purpose of the present document is to provide a framework for enhanced coordination among United Nations entities in response to concerns of Member States regarding cybercrime and cybersecurity. Based on the proposed framework, the High-level Committee on Programmes could consider the possibility of developing further United Nations-wide guidance in the area, which may, for example, take the form of guidance notes, a repository of best practices in the delivery of technical assistance or a full policy based on the framework.

2. For the purposes of the present document, an important distinction is made between the internal and external efforts undertaken by United Nations entities to enhance cybersecurity and combat cybercrime. The focus is solely on the external efforts of United Nations entities concerning Member States. Internal aspects of cybersecurity, including management and administration aspects of cybercrime and cybersecurity risks to the Organization, are addressed by the work of the High-level Committee on Management.[a]

3. The purpose of the framework is:

(a) To highlight the intersections between United Nations entity mandates and activities related to cybercrime and cybersecurity areas, with a view to strengthening support to Member States across a range of technical assistance areas, including information and communications technology (ICT) development, governance, education, health, child protection, financial systems, criminal justice and crime prevention;

(b) To facilitate programme development and technical assistance within the United Nations system, to promote increased efficiency and effectiveness in the early warning, detection and analysis of cyberthreats and the investigation, prosecution, and adjudication of cybercrime acts, leading to more effective prevention, greater deterrence and more just outcomes for suspected persons, in line with international human rights standards;

---

[a] The United Nations Chief Executives Board for Coordination special interest group on information security has developed guidelines, including information security measures and controls, to help United Nations agencies that are owners and operators of critical infrastructure to identify, assess and manage cyberrisk. In accordance with those guidelines, actions taken to mitigate cybercrime risk should identify those areas for improvement that could be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for differences within the United Nations Organization, competent bodies should provide guidance that is technology-neutral and that enables United Nations agencies to benefit from a competitive market for products and services that meet the standards, methodologies, procedures and processes developed to address cyberrisks. The guidelines should include methodologies to identify and mitigate the impacts of cybercrime and associated information security measures or controls on business confidentiality and to protect individual privacy and civil liberties.

(c) To incorporate into the United Nations system technical assistance the importance of cyberthreat risk mitigation in using ICT and the adoption of cyberattack prevention mechanisms by Governments, private-sector organizations and end users, leading to reduced victimization in cyberspace;

(d) To emphasize the importance of best practices and standards that could be adopted in the delivery of technical assistance, aimed at improving cybersecurity management;

(e) To harmonize existing United Nations efforts to encourage effective long-term "whole-of-government" responses to cyberthreats and cybercrime, including national policies, strategies, governance structures, coordinating mechanisms, capacity-building, global standards, data collection systems and effective cybercrime and cyberthreat legal frameworks, leading to a sustainable response and expected greater deterrence;

(f) To promote the delivery of United Nations assistance that strengthens communication between government agencies in cyberthreat, cyberterrorism and cybercrime matters; such assistance should be between the concerned national stakeholders, including ICT policymakers and regulators, judicial systems, civil society, law enforcement bodies, private-sector organizations, civil society and the public, and in international cooperation, leading to increased efficiency and effectiveness of crime prevention and criminal justice response, as well as more effective investments in ICT for sustainable development;

(g) To develop subsidiary specialized frameworks that address different categories of cyberthreats and allow the development of further policies for the delivery of assistance to Member States on particular cybersecurity and cybercrime issues.

4. Section I of the present document establishes common definitions and includes a brief description of the complex scope of cybercrime and cybersecurity. It also provides a conceptual baseline that is referenced throughout the framework document. Section II includes a summary of the intersections between the responsibilities of United Nations entities for cybercrime and cybersecurity and sets out the relevance of mandates and activities of the various entities. Section III establishes the basic principles for programme development related to cybercrime and cybersecurity. It also contains guidance on how United Nations entities could better cooperate in order to deliver products and services to Member States. Section IV contains further elaboration on the core areas for cybercrime and cybersecurity assistance that could be provided to Member States, on the basis of the basic principles in section III. It also contains guidance on some of the topical areas that should be considered for inclusion in related programmes of Member States.

I. Establishing a common understanding of cybercrime and cybersecurity

5. There exists a range of varying definitions of cybercrime.[b] However, common themes include crimes against the confidentiality, integrity and availability of computer data and ICT systems as well as ICT-supported critical infrastructure; computer-related acts for personal or financial gain or harm; and computer content-related acts.

6. Definitions of cybersecurity also vary. In its recommendation X.1205, the International Telecommunication Union (ITU) establishes an agreed definition of cybersecurity as the collection of tools, policies, laws, regulations, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the establishment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality
- Resilience
- Incident prevention

7. In its standard ISO 17799, the International Organization for Standardization states that information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. In its standard ISO/IEC 27002, it defines information security as the preservation of confidentiality, integrity and availability of information. Many Governments that have developed specific cybersecurity frameworks have expanded those definitions (e.g. the Cybersecurity Act of 2012 of the United States of America).

[b] A 2013 comprehensive study on cybercrime prepared by the United Nations Office on Drugs and Crime (UNODC) for the open-ended intergovernmental expert group on cybercrime defined cycbercrime as including the following acts: illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal interference with a computer system or computer data; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright or trademark offences; sending or controlling sending of "spam"; computer-related acts causing personal harm; computer-related solicitation or "grooming" of children; computer-related acts involving hate speech; computer-related production, distribution or possession of child pornography; and computer-related acts in support of terrorism offences.

II. Intersections between United Nations entity mandates in cybercrime and cybersecurity

8. The United Nations Office on Drugs and Crime (UNODC) is the lead entity within the United Nations system on drug control, crime prevention and criminal justice matters, and the guardian of the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime and the Protocols thereto. The mandates of UNODC related to cybercrime therefore relate to the crime prevention and criminal justice domain. That includes the delivery of technical assistance to Member States through its global programme on cybercrime in the areas of digital forensics for law enforcement officers; electronic evidence for criminal justice professionals; international cooperation in cybercrime matters; legislation, strategies and government coordination against cybercrime; as well as awareness-raising and cybercrime prevention.

9. ITU is the specialized agency for ICT. It has been identified by the World Summit on the Information Society as the sole facilitator for its action line C5, on building confidence and security in the use of ICT. As one of the outcomes of the World Summit, in its role as facilitator, ITU launched the ITU Global Cybersecurity Agenda to provide a framework within which the international response to the growing challenges to cybersecurity could be coordinated and addressed among various stakeholders (e.g. Governments, the private sector, international organizations, civil society and academia).

10. In May 2011, UNODC signed a memorandum of understanding with ITU for the purposes of cooperation in the delivery of technical assistance in the area of cybercrime and cybersecurity, within the respective mandates of each organization. Pursuant to that memorandum of understanding, UNODC works with ITU in the delivery of technical assistance at the request of Governments. In that context, and as indicated above, the focus of UNODC is on the crime prevention and criminal justice aspects of preventing and combating cybercrime, while the focus of ITU is on enhancing cybersecurity through, inter alia, the protection of critical infrastructure from computer-based attacks.

11. The regional commissions address such issues at the regional level. For example, the Economic and Social Commission for Western Asia (ESCWA), in its regional plan of action for building the information society, identified a need for significant work in the area of cyberlegislation and cybercrime. The plan of action was endorsed by the member countries of ESCWA in its resolution 273. Under that mandate, ESCWA has worked closely with its member countries in those areas. Other organizations also provide similar services in their respective regions.

12. Intersections also exist between the activities and mandates of other United Nations entities regarding cybercrime and cybersecurity. Many wider development programmes, for example, are dependent upon the implementation of available and resilient computer infrastructure within the institutions of Member States. United Nations entity-specific intersections therefore include:

(a) The Food and Agriculture Organization of the United Nations, the International Fund for Agricultural Development and the World Food Programme (WFP), at which cybersecurity ensures the availability of critical information collection and dissemination in rural areas, including alerts regarding damaging weather effects and the collection of information in rural areas;

(b) The International Atomic Energy Agency (IAEA), at which cybersecurity is used to safeguard the safety and security of nuclear installations, equipment and staff, the integrity and availability of incoming data and information from Member States and other parties related to emergency situations and the confidentiality of data and information related to the safeguards programme. The work of IAEA on cybersecurity has previously focused on building awareness and Member State capacity, primarily for the protection of nuclear material. IAEA is currently broadening that scope to include projects related to crime scene investigation and forensics at nuclear/radiological facilities following a cyberattack;

(c) The Office of the United Nations High Commissioner for Refugees (UNHCR), which collaborates with WFP, the International Federation of Red Cross and Red Crescent Societies, the United Nations Children's Fund (UNICEF), the World Health Organization and other agencies in the provision of integrated humanitarian support for refugees and other affected populations using smart identification card technology based on international standard public-key infrastructure for identification, cash management, medical, schooling, non-food items and other purposes;

(d) The Office of the United Nations High Commissioner for Human Rights which monitors computer-related acts involving advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; child pornography; the protection of the right to privacy, freedom of expression, information and association; the prohibition of sexual exploitation and abuse and of incitement to racial discrimination; and advancement of the fair administration of justice and redress for victims;

(e) UNICEF, which is the lead agency within the United Nations system for child protection and which monitors the protection of children from all forms of violence, abuse, exploitation and discrimination facilitated through information and communications technology;

(f) The United Nations Development Programme and the World Intellectual Property Organization, which monitor activities with regard to computer-related acts for personal or financial gain or harm, e-governance and corruption;

(g) The United Nations Conference on Trade and Development (UNCTAD), which is the lead capacity-building provider within the United Nations system to support the preparation of legal frameworks for e-commerce in developing countries, in accordance with its mandate since 2000. UNCTAD has a long history of supporting developing countries and regions. Through its e-commerce and law reform programme, policymakers and lawmakers (including parliamentarians) from about 30 developing countries in Africa, Asia and Latin America have benefited from capacity-building workshops that have enabled them to prepare and enact e-commerce frameworks. Comparative studies for cyberlaw harmonization have been conducted for the East African Community, Latin America, Central America and the Association of Southeast Asian Nations. Key issues include electronic transactions, electronic signatures and authentication, data protection and privacy, consumer protection, computer crime, intellectual property, competition, taxation and information security at large;

(h) The United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women) promotes the benefits of ICT for the empowerment of women

and girls while simultaneously raising awareness of the need to combat new threats, including online violence against women. Through its partnership with public, private and civil society actors, UN-Women promotes the incorporation of gender perspectives and the participation of women in ICT policies, Internet governance, social responsibility in the use of ICT, the establishment of regulations, codes of conduct and legislation and complaint and monitoring mechanisms;

(i) The World Bank supports Member States in the areas of investment in ICT infrastructure and providing technical assistance in developing policy, legal and regulatory enabling environments, training and capacity-building.

13. A detailed list of the mandates of United Nations entities is provided in a compendium on United Nations mandates on cybersecurity and cybercrime, prepared for the benefit of all United Nations entities. The compendium should be considered a living document and United Nations entities are requested to provide regular updates to it by e-mail.

III. Basic United Nations-wide principles applicable to cybercrime and cybersecurity

14. The first United Nations-wide principle on cybercrime and cybersecurity is that cyberincidents should be dealt with in a holistic manner through the delivery of technical support for criminal justice and the strengthening of international cooperation in prevention, identification, investigation response, prosecution and recovery. Cybercrime and cybersecurity concerns should be addressed as a continuum that integrates both cybersecurity as an important approach to cybercrime prevention and a robust criminal justice response to cybercrime that supports effective cybersecurity. United Nations entities, where possible, should therefore aim to strengthen cybersecurity by establishing prevention mechanisms through capacity-building and awareness-raising and by offering technical support for enhancing response capabilities and for ensuring data recovery and business continuity.

15. The second principle is that United Nations entities should aim to respond to cybercrime and cybersecurity needs in Member States within their respective mandates. In connection with defining specific interventions, they should assess and review possible cybercrime and cybersecurity elements within relevant technical support programmes and country requests for assistance and, where such elements are identified, United Nations entities should consider whether needs should be addressed in coordination and cooperation with other relevant entities.

16. The third principle is that all cybercrime and cybersecurity-related programming by United Nations entities should respect the principles of the rule of law and human rights, the rights to privacy, freedom of expression, information and association, the prohibition of sexual exploitation and abuse and of incitement to racial discrimination, and the advancement of the fair administration of justice and redress for victims. Human rights are at the core of all work of the United Nations system and, together with peace and security as well as development, represent one of the three, interlinked and mutually reinforcing pillars of the United Nations, as enshrined in its Charter. A human rights-based approach should be mainstreamed into the approach of Member States to cybercrime and cybersecurity-related issues.

17. The fourth principle is that cybercrime and cybersecurity programming by United Nations entities should focus on assisting Member States to take evidence-based action, supported by a crime and risk assessment of a potential threat, taking into consideration particular responses to regional or national risk factors.

18. The fifth principle is that, where possible, cybercrime and cybersecurity-related programming should foster a "whole-of-government" response. Such responses may include training and human capacity-building for key national stakeholders, such as law enforcement officers, criminal justice officials, ICT regulators, policymakers, legislators and cybersecurity experts, as well as creating policies, infrastructure and procedures aimed at strengthening cybersecurity. Training and capacity-building activities should also include non-State actors such as non-governmental organizations, academia and the technical community.

19. The sixth principle is that support to Member States should, where possible and bearing in mind the sovereign rights of Member States, aim to strengthen relevant formal and informal mechanisms for international cooperation in cybercrime and cybersecurity matters, with a view to taking into account the global cross-border nature of cybercrime and cybersecurity threats.

20. The seventh principle is that cybercrime- and cybersecurity-related programming should include efforts to strengthen cooperation between government institutions and private-sector enterprises, including suppliers of electronic communication networks and services and financial services institutions. Such cooperation is important in order to properly manage backbone infrastructure, including such issues as resilience, industrial control systems, identity management, Internet root name server administration and spam regulation. Harmonization and the adoption of technical policy and security standards and guidelines at the regional and international levels should be supported.

IV. Assistance areas relevant to cybercrime and cybersecurity

A. Legal measures

21. The establishment of appropriate legal structures is an integral component of national cybersecurity and cybercrime strategies. Initiatives to combat cybercrime and strengthen cybersecurity should be placed within a strong legal framework compatible with the rule of law and international human rights standards.

22. Assistance should be provided to Member States, especially developing and least developed countries, consistent with their maturity levels and local needs, to establish a sound legal basis for a robust cyberregulatory environment (e.g. personal data protection, e-transactions, e-signature and e-commerce). A selected legislative approach should be harmonized with relevant regional and global mechanisms, and consistent with the principles of bilateral legal cooperation among and between Member States.

23. With respect to cybercrime laws, assistance can be delivered by taking into account different legal approaches with regard to substantive criminal law, procedural law, jurisdiction, international cooperation and the responsibility of Internet service providers, including examples of international approaches, as well as examples of best practices from national solutions. United Nations entities should

share and benchmark existing comprehensive and holistic legislative frameworks in order to facilitate national approaches to cybercrime and cybersecurity and facilitate building blocks for organizing national cybercrime and cybersecurity efforts.

24. Assistance should focus on supporting a crime prevention and criminal justice framework that is holistic, technology-neutral and flexible. The objective should be to strengthen the rule of law through the prevention of cybercrime and the promotion of fair, humane and accountable criminal justice systems in line with the United Nations standards and norms in crime prevention, criminal justice and human rights.

B. Policy and strategy measures

25. Cybercrime and cybersecurity policies and strategies may form part of a wide range of policy initiatives at the national level, ranging from overall ICT policies and strategies to national security or infrastructure policies and strategies, as well as crime prevention policies and strategies. Where possible, United Nations entities offering support to the development of a national policy or strategy should seek opportunities for the inclusion of cybercrime and cybersecurity perspectives, where appropriate, in close cooperation with other relevant United Nations entities.

26. National cybercrime and cybersecurity policies and strategies should take into account the obligations of government and private-sector institutions in order to achieve a balanced and comprehensive approach to cybersecurity and the prevention and combating of cybercrime. On the basis of the present framework, United Nations entities should engage in further research and analysis with a view to further identifying possible best practices in this respect, with the public interest as paramount.

27. With respect to cybersecurity, United Nations entities should support the development of national policies and strategies that establish a model of governance for cybersecurity purposes, including defining a common security baseline. United Nations entities should help Member States to create a common legal and regulatory framework, including the criminalization of cybercrime, and to establish a system for the regular updating of policies and strategies to address the changing nature of security threats. Such strategies should also include the establishment of related standards and best practices.

28. In particular, with respect to cybersecurity, policy considerations that should be incorporated into national strategies should include active steps to prevent cybercrime by reinforcing the security of existing critical infrastructure systems. Those steps should include proactively designing systems with principles of cyberattack prevention and resiliency in mind. The integration of applicable global standards for information system security should be considered as a matter of priority at the national, regional and global levels. Relevant stakeholders may also wish to carefully evaluate the value of policies for establishing preventative measures at the consumer level, through programmes that promote safer computing practices, educational campaigns and the provision of anti-malware software packages.

29. With respect to cybercrime strategies, a critical component of the response to cybercrime involves building trust both between national law enforcement and

criminal justice authorities and between law enforcement authorities, the private sector and the public. National cybercrime strategies should include, as appropriate, strategies on awareness-raising, international cooperation, the development of law enforcement and criminal justice capacity, cybercrime legislation, cybercrime prevention and the strengthening of public-private partnerships.

30. Effective cooperation at the international level can be improved by:

- National and regional legal frameworks that approach the criminalization of cybercrime acts in harmonized ways and provide for specialized law enforcement investigative measures
- The application of model legislation that can assist in achieving the harmonization and interoperability of legislative approaches
- International and regional treaties, conventions and agreements, which Member States should consider being party to as part of their multi-lateral cybersecurity and cybercrime efforts
- Information exchange, specifically in relation to sharing major incident reports through a cooperation platform that allows fast and effective exchange of relevant critical information related to cyberthreats and cyberattacks

C. Technical measures

31. Compared with conventional crimes, the involvement of a computer, mobile phone or computer data in a crime event presents some key challenges, such as access to evidence (since cybercrime is in electronic form, lifetime and location may vary); handling evidence (maintaining necessary standards for use in court); and identifying the perpetrator (collaboration among investigation authorities, if the perpetrator is located in a different country).

32. Technical assistance on cybercrime prevention and cybersecurity should be delivered in response to specific individual country needs and based on the results of a comprehensive in-country assessment completed prior to commencement of any activities.

33. United Nations agencies should support the harmonization of technical cybersecurity policy and security standards on an international scale. In that regard, standard development bodies have a vital role to play in addressing security vulnerabilities and greater participation of the private sector and Governments in their work should therefore be encouraged.

34. United Nations agencies should establish an information-sharing mechanism through the creation of a common repository of cybercrime and cybersecurity best practices, which would help other organizations to undertake their mandates. Pursuant to resolution 22/8 of the Commission on Crime Prevention and Criminal Justice, a UNODC central data repository on cybercrime legislation, case examples, best practices and lessons learned is currently under development.

35. Support should be given to the development of technical publications on issues such as comprehensive assessments of the capacity of countries to prevent and combat cybercrime and improve cybersecurity; international cooperation in cybercrime and cybersecurity; the role of digital computer forensic evidence in the prosecution and

adjudication of cybercrime and statistical approaches to measuring and monitoring cybercrime; the level of maturity and readiness of countries, as well as guides and toolkits on relevant legal frameworks, technical measures and standards; the establishment of national cybersecurity policies and strategies, including the development of related incident response capabilities (such as computer incident response teams); and the provisions of international, regional and national human rights law applicable to the prevention of and criminal justice response to cybercrime.

36. United Nations entities should develop programmes to help law enforcement work with ICT service providers in order to obtain relevant digital computer forensic evidence in a timely manner using appropriate methodologies. This may include the establishment of online reference databases on matters of private-sector cooperation to support best practices in searching for and obtaining computer forensic evidence, as well as standard formats for the submission of requests for electronic evidence in the process of international cooperation in criminal matters.

37. United Nations entities should develop programmes designed to assist policymakers and government officials with developing comprehensive strategies and measures addressed at protecting government data, systems, networks and critical infrastructure.

38. United Nations entities should also engage in supporting recovery efforts by Member States after a cyberattack, as dictated by their specific mandates.

D. Capacity-building

39. A comprehensive and holistic approach to cybercrime requires preventive capacity-building in human development. The concept of prevention is grounded in the notion that crime and victimization are driven by many causal or underlying factors. Those are the result of a wide range of circumstances that influence the lives of individuals and families and of local environments, situations and opportunities that facilitate victimization and offending. Good crime-prevention practice starts with basic principles, such as leadership, cooperation and the rule of law, suggests forms of organization, such as a crime prevention plan with clear priorities, targets and goals, and leads to the implementation of methods, such as development of a sound knowledge base and approaches, including reducing criminal opportunities and target hardening.

40. Within that context, particular preventative strategies for addressing cybercrime can include:

(a) Awareness-raising among potential victims and enforcement authorities regarding online dangers and initiatives that can be implemented to minimize risks. User education to achieve high levels of security-conscious behaviour is a critical measure. Recommendations may include helping users to choose secure but memorable single sign-on passwords at a convenient time; emphasizing that passwords will never be requested in a telephone call or e-mail or after clicking on a link in e-mail messages; and campaigns directed at women who are subjects of online or computer facilitated violence and threats;

(b) Cooperation between Governments, police authorities and the private sector, such as Internet service providers and domain name system service providers, to explore technical steps that can be taken to minimize threats. Internet

service providers have a privileged view of all traffic passing to and from their clients' hosted services and have the technical ability to prevent the illegal use of services. Restrictions are usually placed on the nature of services through service agreements, which often cover the most significant types of abusive behaviour. Internet service providers can thus play a role in cybercrime prevention in two main areas: through the storage of user data that can then be accessed and used by law enforcement in cybercrime investigations; and through appropriate measures regarding Internet content and communications, taking into account national and international laws and standards on data protection and human rights with a view to preventing cybercrime acts;

(c) Research and profiling of cybercrime markets and the nature of individuals and organized criminal groups involved, with a view to early intervention;

(d) Increased research and understanding of the underlying economics of cybercrime, including both direct and indirect costs. Direct costs can relate to money withdrawn from victims' accounts, time and effort to reset account credentials or repair computer systems and secondary costs, such as charges for overdrawn accounts. Indirect costs are the monetary equivalent of losses imposed on the society by cybercrime, such as loss of trust in online banking and "defence costs" of cybersecurity products and services. Research on economic and monetary flows associated with cybercrime, such as illicit markets for the sale or rent of computer misuse tools or stolen financial information, may also offer important starting points for law enforcement investigations.

41. Consistent with the above-mentioned second principle on cybercrime and cybersecurity, all cybercrime technical assistance, including the areas of prevention, capacity, frameworks and cooperation, at the international, regional and subnational levels, should be delivered in a collaborative manner by different United Nations entities, according to their respective mandates, in response to specific individual country needs and based on the results of a comprehensive in-country assessment completed prior to commencement of any activities.

42. Approaches to increasing digital investigation capacity should be guided by a focus on team-building between investigators and prosecutors, emphasizing the handling of all evidence in a forensically sound manner that preserves the integrity of evidence for later admission in legal proceedings. Where possible, cybercrime investigation training should follow a train-the-trainer format that begins with providing training to key cybercrime unit members who can then develop a long-term and sustainable programme for developing local capacity. Training, specifically when addressing such fundamental topics as data acquisition and analysis, should be delivered using teaching methodologies that engage participants in an interactive format with hands-on practical exercises that require participants to demonstrate an understanding of key concepts and apply basic skills. Fictional case evidence and fact patterns may be utilized as a teaching methodology to test participants' ability to apply their new skills in potential real world case problems. Core skills for cybercrime training should be adapted to address the most common forms of cybercrime encountered by law enforcement in the specific region and may include, desktop, mobile and network forensics as well as basic core analog skills, necessary for seizing evidence and presenting it effectively in legal proceedings. All training should be delivered in partnership with committed local organizations that provide local facilitation, support and ownership, and should be designed as a sustainable,

ongoing effort that builds local capacity through continuing local management, long-term partnerships and collaboration.

43. Similarly, capacity-building needs to be promoted in order to develop a sustainable and proactive culture of cybersecurity. Within this context, strategies include the following:

(a) The promotion of cybersecurity culture for all stakeholders who develop, own, provide, manage, service or maintain information networks, whereby those stakeholders understand cybersecurity issues and take action appropriate to their roles in order to protect networks. Such efforts could be done through the development of appropriate guidelines on how to raise awareness on cybersecurity issues for small and medium-sized enterprises, consumers and end users. Governments should take a leadership role in promoting cybersecurity culture and in supporting the cybersecurity and cybersafety efforts undertaken by other stakeholders;

(b) Encouragement of national Governments to lead national efforts to carry out regular self-assessments of their existing national policies, procedures, norms, institutions and relationships in the light of national needs to enhance cybersecurity, including critical information infrastructure protection. Cybersecurity, including critical information infrastructure protection, are responsibilities that are shared by Government, business, other organizations and individual users, who develop, own, provide, manage, service or use information systems and networks. Managing inherent security risks requires the active cooperation of all participants, addressing the security concerns relevant to their roles. The collective goal is to prevent, prepare for, respond to and recover from any incidents rapidly, while minimizing damage;

(c) Support for training and for building and deploying the technical capabilities of national computer incident response teams, for them to serve as trusted, central coordination points of contact for cybersecurity, aimed at identifying, defending, responding and managing cyberthreats.

E. Cooperation among stakeholders

44. The facilitation of working relationships between key stakeholders at the international, regional and national level is critical for fighting cybercrime and achieving improved cybersecurity. Efforts should be made to focus, where possible, on strengthening existing programmes and designing new programmes that reinforce mechanisms for cooperation, both formal (such as bilateral or multilateral agreements on mutual legal assistance) and informal (through initiatives by various international or regional entities). Activities should include the implementation of information-sharing mechanisms between law enforcement agencies and the private sector, as well as corporate procedures and due legal process requirements for enabling information-sharing.

45. United Nations programmes aimed at supporting the efforts of Member States to enhance international and regional cooperation should deliver technical advice by international and national experts on relevant measures, such as the establishment of domestic fast-response/expedited focal points and mechanisms to coordinate domestic activities, and serve as central contact points for requests from abroad. The focal points and mechanisms should, where possible, be established within existing frameworks of mutual legal assistance agreements and extradition-competent

authorities. In that regard, the provision of updated background and contact information of focal points to existing databases maintained by relevant United Nations agencies should be encouraged.

46. Technical advice should be provided with regard to the establishment of informal cooperation focal points and mechanisms, tailored to the specific internal organizational structures of Member States, for addressing issues of cybersecurity and cybercrime.

47. United Nations entities should aim to facilitate, within their respective mandates and areas of responsibility, improved cooperation and coordination among national stakeholders, in order to avoid duplication of national efforts and foster a more harmonized approach towards the establishment of national policies and strategies.

48. Regional meetings for the purposes of formulating regional and subregional informal and formal cooperation mechanisms should be planned to encourage multi-stakeholder cooperation in investigation and prosecution.

49. Within the context of their respective mandates and areas of responsibility, United Nations entities should establish an appropriate mechanism for:

- Assessing the needs and requirements of Member States in addressing cyberthreats and cybercrimes with a view to maximizing the existing expertise within the United Nations system
- Exploring arrangements among United Nations entities to allow more information exchange and instigate cooperation by sharing resources and expertise
- Establishing measures to cooperate with other international and regional organizations that engage in supporting States in their efforts to combat cybercrime and achieve cybersecurity

V. Mechanisms of framework implementation

50. Efforts should be made to adopt and implement a comprehensive, long-term and holistic approach to preventing and combating cybercrime and to ensure cybersecurity by building on existing domestic frameworks, initiatives, partnerships and standards of United Nations agencies, intergovernmental organizations and civil society, on matters including awareness-raising, reporting, international cooperation, capacity-building and delivery and coordination of technical assistance.

51. There should be a focus on facilitating and enhancing cooperation and developing best practices among Member States within the respective cybercrime and cybersecurity mandates and areas of responsibility of the United Nations entities. Such efforts could be achieved by promoting tools that provide data on best practices and lessons learned, such as data repositories and case law databases, and by conducting meetings, workshops and conferences at the international, regional and national levels, focusing on specific thematic areas and target groups, such as law enforcement officers, members of the judiciary, government experts and other relevant stakeholders. Cybersecurity and cybercrime best practices should be integrated into all relevant programmatic documents, for Member State support.

52. Efforts should be made to integrate best practices into the United Nations Development Assistance Framework to provide support to Member States in a manner that is coordinated with the contributions of other United Nations institutions to such programmes in the area.

53. Efforts should be made to ensure that initiatives are not duplicated and to find complementarities in the mandates of each agency, while clearly identifying the areas of complementary expertise in the work carried out by individual agencies in the field, through the enhancement of appropriate coordination mechanisms among United Nations entities, especially with respect to:

- Exploring the establishment of arrangements among entities aimed at finding complementarities in the mandates of concerned entities, aimed at allowing more information exchange and encouraging cooperation by sharing resources and expertise as a measure of internal capacity-building (including through agreements and memorandums of understanding)
- Appointing clearly identifiable focal points within each agency (e.g. chief information security officers, ICT programme officers or cybercrime and cybersecurity experts) to facilitate more effective coordination on cybercrime and cybersecurity matters[c]
- Conducting needs assessments for Member States
- Exploring the establishment of joint programmes, such as computer incident response teams and information-sharing and analysis centres

54. A framework should be adopted for mitigating cyberrisk in order to reduce cyberrisks to critical infrastructure. The framework should include a set of standards, methodologies, procedures and processes that align policy, business and technological approaches to address cyberrisks. Broad standards and industry best practices should also be adopted by United Nations agencies to the fullest extent possible, as applicable to their current standards and operational risk tolerance.

55. United Nations entities should develop the capacity to analyse the programme impact of cybersecurity and cybercrime on their programme activities.

[c] During its first meeting, the group decided to adopt the terms of reference of the members of the United Nations focal points on cybercrime and cybersecurity. The terms of reference affirm that: (a) each international organization would appoint a focal point responsible for policy development in the domain of cybercrime and cybersecurity. The focal point would act as member of the group and liaison with his/her organization; (b) it would be recommended to appoint focal points primarily with a background on programme policy aspects of cybercrime and cybersecurity. However, due to the different mandate and expertise of the different United Nations agencies, each organization would be responsible for appointing any focal point that could be relevant for the scope and work of the group.