A. Introduction

1. The first, second and third substantive sessions of the Open-ended Working Group (OEWG) on the security of and in the use of Information and Communications Technologies (ICTs) 2021–2025 took place in a challenging geopolitical environment with rising concern over the malicious use of ICTs by State and non-state actors. At these sessions, States recalled the contributions of the first OEWG on this issue, established pursuant to General Assembly Resolution 73/27, which concluded its work in 2021. Furthermore, States reaffirmed the consensus report of the 2021 OEWG on developments in the field of ICTs in the context of international security and took note of the consensus reports of the groups of governmental experts (GGEs) of the 2010, 2013, and 2015, and 2021 groups of governmental experts (GGEs). States recalled and reaffirmed also noted that the reports of these groups “recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time”, and that “specific confidence-building, capacity-building and cooperation measures were recommended”. States also recalled and reaffirmed that “international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment”. These elements consolidate an initial framework for responsible State behaviour in the use of ICTs, providing a foundation which could be built upon. States also noted the consensus resolutions of the General Assembly on developments in the field of information and telecommunications in the context of international security. In this regard, the OEWG also noted General Assembly resolutions 73/27 and 75/240, in which States agreed they should be guided in their use of ICTs by the OEWG and GGE reports.

2. The OEWG recalled its mandate contained in General Assembly resolution 75/240 as follows: “Acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour; to consider initiatives of States aimed at ensuring security in the use of information and communications technologies; to establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States; to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, *inter alia* data security, and possible cooperative measures to prevent and counter such threats; and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building; and to submit, for adoption by consensus, annual progress reports and a final report on the results of its work to the
General Assembly at its eightieth session.” In this regard, the OEWG acknowledged the importance of addressing its mandate in a balanced manner and the need to give due attention to both further develop common understandings between States on the use of ICTs, as well as to further the implementation of existing agreements.

3. The OEWG is committed to engaging stakeholders in a systematic, sustained and substantive manner, in accordance with the modalities agreed by silence procedure on 22 April 2022 and formally adopted at the first meeting of the third session of the OEWG on 25 July 2022, and in line with its mandate contained in General Assembly Resolution 75/240 to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia. While different views were expressed on the preferred modalities to be adopted, the eventual agreement was a positive step that demonstrated flexibility on the part of all delegations.

4. The OEWG recognized that regional and sub-regional organizations have made significant efforts in the field of security in the use of ICTs. In addition, regional, cross-regional and inter-organizational exchanges can establish new avenues for collaboration, cooperation, and mutual learning. As not all States are members of a regional organization and not all regional organizations focus on the issue of security in the use of ICTs, the OEWG noted that regional efforts are complementary to the work of the UN and other organizations on this issue.

5. The OEWG welcomed the high level of participation of women delegates in its sessions and the prominence of gender perspectives in its discussions. The OEWG underscored the importance of narrowing the “gender digital divide” and of promoting the effective and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security.

6. In recognition that the OEWG is in the early stages of its deliberations and substantive discussions under the OEWG will continue until the completion of its mandate in 2025, this first annual progress report of the Group is not intended to be a comprehensive summary of discussions by States which are ongoing, but aims to capture concrete progress made at the OEWG to date, with a focus on the proposals by States as well as and next steps of the OEWG, as well as set out a roadmap for focused discussions on specific topics within the OEWG’s mandate. This progress report will be submitted to the General Assembly pursuant to the OEWG mandate in resolution 75/240.

B. Existing and Potential Threats

7. States made concrete, action-oriented proposals to address existing and potential threats. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions.

   a) States, recalling the threats identified in the 2021 OEWG report, reiterating increasing concern that threats in the use of ICTs continue to intensify and evolve, and underscoring the implications of the malicious use of ICTs for the maintenance of international peace and
security, proposed that the OEWG, as a UN inter-governmental body, could be a platform to foster global, inter-regional cooperative approaches on security in the use of ICTs.

b) Bearing in mind the interrelated and mutually-reinforcing nature of the pillars of the OEWG’s mandate, States proposed technical and cooperative measures to address existing and potential threats with regard to security in the use of ICTs through appropriate fora, including:

(i) Cooperation and assistance to establish and strengthen Computer Emergency Response Teams (CERTs);
(ii) Developing and disseminating comprehensive best practices on the classification and protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII);
(iii) Cooperation and assistance to ensure the integrity of the supply chain, and prevent the use of harmful hidden functions;
(iv) Sharing, on a voluntary basis, of risk assessments and technical information between States including relevant threat intelligence and compendiums;
   (iv Bis) Establishing a glossary of terms for common use.
(v) Cooperation and assistance for developing ICT security baseline studies and designing security as a critical requirement;
(vi) Sharing of risk assessments and technical information between States including threat intelligence and compendiums; [text moved above]
(vii) Developing and disseminating comprehensive best practices on the classification and protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII). [text moved above]
   (vi) Undertaking international exercises and technical training for policymaking personal including of law enforcement officials in coordination with other relevant processes and entities;
   i (vii) Prioritizing capacity building and technical assistance, including mutual legal assistance in coordination with other relevant processes and entities;
   ii (viii) Enhancing tailored capacity building efforts;
   iii (ix) Cooperation and assistance to ensure the integrity of the supply chain, and prevent the use of harmful hidden functions; [text moved above]
   iv (x) Measures and initiatives to strengthen data security
   i (l) (x) Measures to safeguard the general availability and integrity of the internet

c) The OEWG could be a platform to foster global, inter-regional cooperative approaches on the security of and in the use of ICTs. [text moved above] States proposed that there is value in regional and sub-regional organizations sharing relevant experiences at the OEWG as appropriate.

d) States could consider, where feasible, strengthening interactions with interested stakeholders, including businesses, non-governmental organizations and academia, through inter alia, the exchange of knowledge and best practices on the protection of CI and CII.

Recommended next steps
1. States continue exchanging views at the OEWG on emerging and existing threats to security in the use of ICTs with the potential to impact international peace and security, including developing ICT capabilities for military purposes and cooperative measures to address them.

2. States consider utilizing the framework of the OEWG to further exchange technical information relating to existing and potential threats to security in the use of ICTs, including the sharing of risk assessments, relevant threat intelligence, best practices, and incident mitigation measures, on a voluntary basis. Experts could be invited, after consultations with Member States, to make presentations on these topics to facilitate further discussion.

2 bis. States consider developing within the framework of the OEWG a common terminology to facilitate the process of identifying and facing emerging and existing threats.

2 ter. States consider initiating discussions within the framework of the OEWG on the need for a multilateral mechanism for the attribution of cyber incidents.

3. States engage in focused informal discussions on, inter alia, the emerging and existing threats, including developing ICT capabilities for military purposes and, the protection of CI and CII with representatives from the different regions and sub-regions as well as representatives from interested accredited stakeholders, including businesses, non-governmental organizations and academia, at the fourth and fifth sessions of the OEWG.

C. Rules, Norms and Principles of Responsible State Behaviour

8. States made concrete, action-oriented proposals on rules, norms and principles of responsible state behaviour. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) States consider reviewing existing norms and developing additional ones, as well as, a guidance or checklists on norms implementation, elaborating and building upon the conclusions and recommendations agreed to in previous OEWG and GGE reports, as well as consider developing common understandings on technical ICT terms.

b) States proposed that additional norms could continue to be developed over time, noting that the further development of norms and the implementation of existing norms were not mutually exclusive but could take place in parallel.

c) Information exchange on best practices and cooperation could be enhanced, potentially drawing from models of information sharing in other fields, and could include topics such as
innovation, vulnerability disclosure, the protection of critical infrastructure and cooperation between CERTs, on a voluntary basis.

d) States could consider surveying or voluntarily reporting on their national implementation of rules, norms and principles of responsible State behaviour utilizing, on a voluntary basis, existing avenues and tools such as the National Survey of Implementation, as contained in the recommendations of the 2021 OEWG report,9 and the report of the Secretary-General on developments in the field of ICTs in the context of international security.

e) Regarding the consideration of proposals under this topic, States recalled the recommendation in the 2021 OEWG report that States take note of the list of non-exhaustive proposals made on the elaboration of rules, norms and principles of responsible behaviour of States (annexed to the Chair’s Summary in the 2021 OEWG Report) in future discussions on ICTs within the United Nations, including the possibility of additional legally binding obligations.11

Recommended next steps

1. States continue exchanging views at the OEWG with the aim of developing common understandings on, as well as reviewing existing norms and facilitating the implementation of, rules, norms and principles of responsible State behaviour in the use of ICTs, including on best practices in this regard, and discuss the proposals from the non-exhaustive list in paragraph 8(e) 4e) above, as well as developing further ones, including the possibility of additional legally binding obligations, at the fourth and fifth sessions of the OEWG.

2. Interested States or groups of States are invited to submit working papers to contribute to the development of guidance, checklists and common understandings on technical ICT terms along with other tools to assist States in developing common understandings on as well as facilitating the implementation of rules, norms and principles of responsible State behaviour in the use of ICTs and developing further norms, including the possibility of additional legally binding obligations. Such working papers could facilitate a focused exchange of views at the OEWG.

3. States are encouraged to, on voluntary basis, survey and/or report on their national efforts to implement rules, norms and principles, and share experiences and best practices on norms implementation, including through the report of the Secretary-General on developments in the field of ICTs in the context of international security, as well as Member States may also, on a voluntary basis, use the National Survey of Implementation to structure their abovementioned submissions, and the report of the Secretary-General on developments in the field of ICTs in the context of international security.

D. International Law
9. States made concrete, action-oriented proposals on international law. The following is a non-exhaustive list of proposals **with varying levels of support from States** that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could convene discussions on specific topics related to international law. This may include expert briefings, such as from the International Committee of the Red Cross, to consolidate common understandings on this subject. A non-exhaustive list of topics proposed by States for further discussion under international law includes: Sovereignty; sovereign equality; non-intervention in the internal affairs of other States; peaceful settlement of disputes; to consolidate common understandings on how international law, in particular the principles of the Charter of the United Nations, applies in the use of ICTs; whether gaps in common understandings exist on how international law applies, as well as the possibility of additional legally binding obligations; State responsibility and due diligence; respect for human rights and fundamental freedoms; and principles of International Humanitarian Law such as proportionality, distinction, humanity, necessity. Noting that the development of common understandings on international law remains the exclusive prerogative of States, it was proposed that discussions at the OEWG could benefit from briefings, as appropriate, by experts from the UN, such as the International Law Commission, as well as interested stakeholders including businesses, non-governmental organizations and academia.

b) Recalling the recommendation of the previous OEWG, States could continue to inform the Secretary-General of their sharing of national views and assessments, on a voluntary basis, on how international law applies in the to their use of ICTs to ensure international security, and continue to voluntarily share such national views and practices through other avenues as appropriate. Utilizing, on a voluntary basis, existing avenues and tools such as the UNIDIR Cyber Policy Portal and the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal, as appropriate.

c) Capacity-building efforts on international law should be inclusive and could be strengthened and could include workshops and training courses as well exchanges on best practice at the international, inter-regional, regional and sub-regional levels, as well as draw from the experience of relevant regional organizations as appropriate. It was proposed that, in coordination with other relevant processes and entities, capacities could be developed on issues such as, inter alia, common understanding of criteria for unlawful ICT activities by different States and improving mechanisms of mutual legal assistance for investigating malicious use of ICTs.

**Recommended next steps**

1. States continue exchanging views at the OEWG on how international law applies in the use of ICTs.
2. States engage in focused discussions on topics from the non-exhaustive list in paragraph 9(a) above at the fourth and fifth sessions of the OEWG. Such discussions should include informal briefings from experts in an appropriate format.

3. States are invited to continue to voluntarily share their national views and positions on international law, including through existing mechanisms such as the National Survey of Implementation and the report of the Secretary-General on developments in the field of ICTs in the context of international security.

4. States are, on a voluntary basis, invited to submit, on a voluntary basis, information to the UN Secretariat on potential needs and gaps in capacity-building in the area of international law as well as on existing capacity-building initiatives and opportunities. The UN Secretariat is requested to compile this information submitted by States, to prepare a background paper on needs, opportunities and gaps in the area of capacities relating to international law, and to make a presentation on this topic at the fourth OEWG session.

E. Confidence-Building Measures

10. States made concrete, action-oriented proposals on confidence-building measures (CBMs). The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could agree to establish a global, inter-governmental, points of contact directory on ICTs at the United Nations. States may, on a voluntary basis, provide points of contact (PoCs) at the diplomatic, policy and technical levels with due competence at the national level in ensuring security in the use of ICTs that could be reached in times of urgency, for example through hotlines. Such a directory would respect State sovereignty and be politically neutral. It would be updated regularly, and be secure, operational and complemented by enhanced interaction and cooperation between States as well as capacity-building such as table-top exercises where requested. The UN Secretariat could be requested to collect and disseminate to the OEWG best practices on operationalizing such a directory which would include experiences at the regional level, as appropriate.

b) Recalling the recommendation of the previous OEWG, States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate, such as could continue to voluntarily share white papers, national strategies and policies including ICT capabilities as well as share information on national ICT institutions and structures, and national lists of CI. The report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal could be avenues an avenue for the voluntary sharing of such information.
c) It was proposed that aspects of confidence-building could include, where feasible, stakeholder engagement such as cooperation with interested accredited stakeholders, as appropriate, including businesses, non-governmental organizations and academia, on, inter alia, ensuring the integrity of the supply chain, preventing malicious uses of ICTs tools and techniques, preventing the use of harmful hidden functions and the sharing of current threat information. Points of Contact in the private sector could be established as appropriate.
d) Cooperation between CERTs could serve as a confidence building measure which may be strengthened and which includes the sharing and dissemination of good best practices on incident management. Cooperation to mitigate attacks on CI and other malicious ICT-related activity could also be enhanced.
e) States also made a variety of proposals for new CBMs on issues such as, inter-alia, public-private partnerships; the coordinated disclosure of vulnerabilities; the development of common-understanding on a glossary of basic terms with the aim of reducing mistrust by building common understanding; and on the use of ICTs for the economic development of States in a fair and non-discriminatory environment. States continued to emphasize that the OEWG itself served as a CBM.

Recommended next steps

1. States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs.

2. States engage in focused discussions on inter-alia: (a) the development and operationalization of the agreement to establish a global, inter-governmental, points of contact directory and, at the fourth and fifth sessions of the OEWG, to engage in further focused discussions on the operationalization of such a directory on a consensus basis, as well as engage in discussions on related initiatives for related capacity-building and the sharing of best practices, taking into account available best practices such as (b) the sharing of regional and sub-regional experiences where appropriate, on the development and operationalization of CBMs, including briefings by regional and sub-regional organizations as appropriate, at the fourth and fifth sessions of the OEWG.

3. The UN Secretariat is requested to collate compile best practices on the operationalization of a global inter-governmental points of contact directory, which could include experiences at the regional and sub-regional levels, and produce a report with options for the development operationalization of such a global directory by the end of January 2023 for consideration at the fourth session of the OEWG.

4. States are encouraged to submit, on a voluntary basis, information on their national POCs as part of their also voluntary responses to either (a) the report of the Secretary-General on developments in the field of ICTs in the context of international security the National Survey of Implementation, and/or (b) the National Survey of Implementation. The report of the Secretary-General on developments in the field of ICTs in the context of international security.

5. States are invited to submit to the UN Secretariat, on a voluntary basis, their views, suggestions and recommendations on the development of voluntary protocols, procedures, and standardised templates for exchange of information between points of contact at the technical and political levels. The UN Secretariat is requested to collate compile and circulate all submitted information to delegations for discussion at the fourth session.

6. The OEWG Chair is requested to convene an informal inter-sessional meeting with States and interested accredited stakeholders, including businesses, non-governmental organizations and academia, no later than the beginning of the fourth session, to explore the development and implementation of CBMs discuss topics which could support and foster confidence-building, including, inter alia, ensuring the integrity of the supply chain,
preventing malicious uses of ICTs tools and techniques, preventing the use of harmful hidden functions and the sharing of current threat information.

7. States are encouraged to continue, on a voluntary basis, to share relevant information, white papers, national strategies and policies including ICT capabilities as well as information on ICT institutions and structures, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate.

F. Capacity-Building

11. States made concrete, action-oriented proposals on capacity-building. This The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could encourage the mainstreaming of the principles of ICT capacity-building as adopted in the 2021 OEWG report: as well as better integrate ICT capacity-building efforts into the 2030 Sustainable Development Agenda. The Group recognized the different situations, capacities and priorities of States and regions, but also that States have both individual and shared responsibilities in the ICT domain.

b) The OEWG could promote better understanding of the needs of developing States taking into consideration information submitted, on a voluntary basis, by Members States, with the aim of narrowing the digital divide, for instance through encouraging participation in the discussion of the development and use of questionnaires, the National Survey of Implementation; the Cybersecurity Capacity Maturity Model; technical studies; and needs assessment models. Such efforts could also assist in matching needs with resources and lead to more effective coordination in capacity-building.

c) The OEWG could play a role in furthering capacity-building coordination by encouraging coordination between online portals, consolidating and compiling a calendar of capacity-building programmes, and developing a list of regional and sub-regional centres of excellence on security in the use of ICTs to ensure that States, in particular developing States, have timely information and access to such programmes, and encouraging and facilitating unrestricted access of all States to ICT related products, services, equipment, networks, science and technologies. There is a need to guarantee that States and companies refrain from measures hindering the States access to benefits of ICTs.

d) States could consider establishing a permanent multilateral mechanism for exchanging views and ideas related to capacity-building in ICTs, including cyber security training and education, transfer of technology, technical assistance and financial support while taking into account in collaboration and coordination with other existing initiatives. It was proposed that such a mechanism could be established within the UN.
e) States could consider further avenues of funding for ICT capacity-building on security in the use of ICTs through potential coordination and integration with larger development programmes and multi-donor trust funds. In this regard, States also highlighted the possibility of a dedicated trust fund for ICT capacity-building projects for developing States.

f) States could continue to raise awareness of the gender dimensions of ICT security and promote gender-sensitive capacity building at the policy level as well as in the selection and operationalization of projects.

g) States could strengthen coordination and cooperation between States and interested stakeholders, as appropriate, including businesses, non-governmental organizations and academia. States noted that stakeholders are already playing an important role through partnerships with States for the purposes of training public officials, research, and facilitating access to internet and digital services.

Recommended next steps

1. States continue exchanging views at the OEWG on capacity-building.

2. States engage in focused discussions on, inter alia: (a) funding for ICT capacity-building through potential coordination and integration with larger development programmes and multi-donor trust funds as well as a possible dedicated trust fund for ICT capacity building, (b) a permanent mechanism, potentially within the UN, and in collaboration and coordination with other existing initiatives, for exchanging views and ideas related to capacity-building in ICTs while taking into account existing initiatives, including cyber security training and education, transfer of technology, technical assistance and financial support at the fourth and fifth sessions of the OEWG, and (c) best practices and lessons learnt on the topic of public-private partnerships in the use of ICTs at the fourth and fifth sessions of the OEWG. Experts could be invited to make presentations on these topics to facilitate further discussion.

3. States engage in focused discussions on the gender dimensions of ICT security and best practices on how to incorporate the gender dimension in ICT-related projects, for instance how gender-disaggregated participation records and other data can be effectively collected and utilized. Experts could be invited to make presentations on these topics to facilitate further discussion.

4. States are invited, on a voluntary basis, to provide the UN Secretariat with information on forthcoming capacity-building programmes as well as information on regional and sub-regional ICT centres of excellence. The UN Secretariat is requested to make this information available on the OEWG website. [Text moved below]
4. The UN Secretariat is requested to designate an ICT capacity-building focal point with the responsibility of fostering the coordination of coordinating offers and requests for capacity-building, working in collaboration with other UN entities and relevant organizations, taking into account the proposals in paragraphs 11(a)-(g). The focal point could also encourage the coordination of coordinate capacity-building efforts by working, as appropriate, with interested stakeholders, including businesses, non-governmental organizations and academia.

5. States are encouraged, on a voluntary basis, to survey their capacity needs including through the National Survey of Implementation and/or the Cybersecurity Capacity Maturity Model.

6. States in a position to do so are invited to continue to support capacity-building programmes, including in collaboration, where appropriate, with regional and sub-regional organizations and other interested stakeholders, including businesses, non-governmental organizations and academia.

7. States are invited, on a voluntary basis, to provide the UN Secretariat with information on forthcoming capacity-building programmes as well as information on regional and sub-regional ICT centres of excellence. The UN Secretariat is requested to make this information available on the OEWG website.

8. The UN Secretariat is requested to invite interested stakeholders, including businesses, non-governmental organizations and academia, to submit offers to share resources in support of international capacity-building efforts, such as, inter alia, expertise, information, data, experience and training, technical assistance and technology transfer, and to compile information on these offers and share the information on the OEWG website.

G. Regular Institutional Dialogue

12. States made concrete, action-oriented proposals on regular institutional dialogue. This non-exhaustive list of proposals with varying levels of support from States may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could play a role in raising awareness, building trust and deepening understanding in areas where no common understanding has yet emerged. Furthermore, each OEWG session should build incrementally on the previous one. States underlined the centrality of the OEWG as the negotiation mechanism within the United Nations on the security of and in the use of ICTs in the context of international peace and security.

b) States noted a variety of proposals for advancing responsible State behaviour in the use of ICTs, which would, inter alia, support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action (PoA). In considering these proposals, the concerns and interests of all States should be taken into account through equal State participation at the United Nations. In this regard, it was recalled that the PoA should
be further elaborated including at the 2021-2025 Open-Ended Working Group process.16 In considering proposals under this topic, States recalled the recommendation in the 2021 OEWG report that the Programme of Action (PoA) for advancing responsible State behaviour in ICTs should be further elaborated including at the current OEWG.17 It was proposed that the PoA could be a mechanism to support capacity-building for implementing the framework of responsible State behaviour in the use of ICTs.

**Recommended next steps**

1. States continue exchanging views at the OEWG on regular institutional dialogue, under the auspices of the United Nations, while recognize the inclusive and transparent role of the OEWG as the negotiation mechanism within the United Nations on the security of and in the use of ICTs.

2. States engage in focused discussions on the elaboration of a PoA within the framework of the OEWG, including with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, which would, inter alia, support the capacities of States in implementing commitments in their use of ICTs capacity-building. States will also engage in focused discussions, at the fourth and fifth sessions of the OEWG, on the relationship between the PoA and the OEWG, and on the scope, content and timeframe for the establishment of a PoA.

3. States in a position to do so to continue to consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the relevant UN processes.18

---

1 A/75/816.  
5 GA resolutions 70/237 and 76/19.  