22 June 2022

Excellency,

I have the honour of addressing you in my capacity as Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), established pursuant to General Assembly resolution 75/240 adopted on 31 December 2020.

The third substantive session of the OEWG will be held at the United Nations Headquarters in New York from 25 July to 29 July 2022. The meeting will be held in-person and will also be webcast on UN WebTV. Information regarding meeting rooms will be communicated in due course by the Secretariat.

Delegations will recall that resolution 75/240 mandates the OEWG to submit, for adoption by consensus, annual progress reports to the General Assembly. In this regard, I am pleased to enclose a **Zero Draft** of the first annual progress report of the OEWG as a starting point for our discussions, with a view to the adoption of the first annual progress report by consensus at the end of the third substantive session.

The Zero Draft is intended to be a balanced text that captures the range of concrete ideas and proposals raised during the first and second substantive sessions. It is also intended to provide a framework for more focused and in-depth discussions on the topics under our mandate. In this sense, the annual progress report will serve as a roadmap for our future work in 2023.

The draft **programme of work** for the third substantive session, structured in line with the agenda adopted at our organizational session (A/AC.292/2021/1) and General Assembly resolution 75/240, is also enclosed. While I have allocated meeting time for two rounds of discussions of the annual progress report, I anticipate that additional informal meetings and informal-informal meetings may be required to find consensus. I have also allocated time for briefings by regional organizations, the United Nations Institute for Disarmament Research (UNIDIR), as well as for the dedicated stakeholder session provided for in the OEWG's agreed modalities for the participation of stakeholders of 22 April 2022.
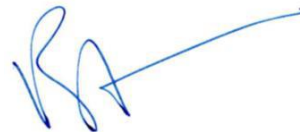
As indicated in my letter dated 15 November 2021, I plan to engage interested stakeholders, including businesses, non-governmental organisations and academia, in an informal consultative meeting ahead of the third substantive session on 21 July 2022. This is a follow-up meeting to the informal consultative meetings that I convened in December 2021 and March 2022.

In order to have a focused discussion with stakeholders, I have prepared guiding questions for both the informal consultative meeting on 21 July 2022 and the dedicated stakeholder session on 27 July 2022. The same guiding questions will be used for both meetings. I intend to write separately to stakeholders to inform them on the arrangements for the two meetings.

I would like to invite delegations to a virtual open-ended informal meeting to hear initial views and reactions to the Zero Draft, and for a briefing on the preparations for the third substantive session on Tuesday, 12 July 2022 at 9.00am (New York time). The Secretariat will disseminate the link for the meeting in due course.

Finally, I would like to invite all Heads of Delegations plus one accompanying expert to an in-person cocktail reception on Monday, 25 July 2022 at 6.30pm at the Permanent Mission of Singapore. The cocktail reception invitation is enclosed.

Please accept, Excellency, the assurances of my highest consideration.

Burhan Gafoor
Chair
Open-Ended Working Group on
security of and in the use of
information and communications
technologies 2021-2025

All Permanent Representatives and Permanent Observers to the United Nations
New York

Enclosures:
- Annex A – Zero Draft of the first annual progress report of the OEWG
- Annex B – Provisional programme of work for the second substantive session
- Annex C – Guiding questions for the informal consultative meeting with stakeholders and the dedicated stakeholder session
- Annex D – Invitation to an in-person cocktail reception at the Singapore Mission on Monday 25 July 2022 at 6.30pm

<u>Zero Draft of 22 June 2022</u>

2022 ANNUAL PROGRESS REPORT OF THE OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES 2021–2025, SUBMITTED TO THE 77TH SESSION OF THE GENERAL ASSEMBLY PURSUANT TO GENERAL ASSEMBLY RESOLUTION 75/240

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 reaffirmed the consensus report of the 2021 OEWG on developments in the field of ICTs in the context of international security[1] and the consensus reports of the 2010, 2013, 2015, and 2021 groups of governmental experts (GGEs).[2] States recalled and reaffirmed 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".[3] States also recalled the consensus resolutions of the General Assembly in which States agreed they should be guided in their use of ICTs by the OEWG and GGE reports.[4]

2. In recognition that 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 next steps of the OEWG. This progress report will be submitted to the General Assembly pursuant to the OEWG mandate in resolution 75/240.

---

[1] A/75/816.
[2] A/65/201, A/68/98, A/70/174 and A/76/135.
[3] Report of the 2021 OEWG, A/75/816, Annex I, para 7.
[4] GA resolutions 70/237 and 76/19.

B. Existing and Potential Threats

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

   a) Technical and cooperative measures to address existing and potential threats, including:
      (i) Cooperation and assistance to establish and strengthen Computer Emergency Response Teams (CERTs);
      (ii) Cooperation and assistance for developing ICT security baseline studies and designing security as a critical requirement;
      (iii) Sharing of risk assessments and technical information between States including threat intelligence and compendiums;
      (iv) Developing and disseminating comprehensive best practices on the classification and protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII).
      (v) Undertaking international exercises and technical training including of law enforcement officials;
      (vi) Prioritizing mutual legal assistance;
      (vii) Enhancing tailored capacity building efforts;
      (viii) Cooperation and assistance to ensure the integrity of the supply chain, and prevent the use of harmful hidden functions;
      (ix) Measures and initiatives to strengthen data security;
      (x) Measures to safeguard the general availability and integrity of the internet.

   b) The OEWG could be a platform to foster global, inter-regional cooperative approaches on the security of and in the use of ICTs. There is value in regional and sub-regional organizations sharing relevant experiences at the OEWG.

   c) States could consider strengthening interactions with interested stakeholders, including businesses, non-governmental organizations and academia, through 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 with the potential to impact international peace and security, 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, including the sharing of risk assessments, threat intelligence, best practices, and incident mitigation measures, on a voluntary basis. Experts could be invited to make presentations on these topics to facilitate further discussion.

3. **States engage in focused discussions on, *inter alia*, the protection of CI and CII with representatives from the different regions and subregions as well as representatives from interested 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

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

   a) States consider developing additional 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.[5]

   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.

   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,[6] 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

---

[5] Report of the 2021 OEWG, A/75/816, Annex I, para 29.
[6] Report of the 2021 OEWG, A/75/816, Annex I, para 65.

responsible behaviour of States (annexed to the Chair's Summary in the 2021 OEWG Report[7]) in future discussions on ICTs within the United Nations.[8]

Recommended next steps

1. **States continue exchanging views at the OEWG on 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 4e) above, 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 the implementation of rules, norms and principles of responsible State behaviour in the use of ICTs. 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, including through 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.**

D. International Law

5. States made concrete, action-oriented proposals on international law. The following is a non-exhaustive list of proposals 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; how international law, in particular 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 proportionality, distinction, humanity, necessity.

---

[7] Report of the 2021 OEWG, A/75/816, Annex II.
[8] Report of the 2021 OEWG, A/75/816, Annex I, para 33.

b) Recalling the recommendation of the previous OEWG,[9] States could continue sharing national views on how international law applies in the use of ICTs, 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.

c) Capacity-building efforts on international law 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. It was proposed that 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 5a) above at the fourth and fifth sessions of the OEWG. Such discussions should include briefings from experts.**

3. **States are invited to continue to voluntarily share their national views 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 information to the 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 Secretariat is requested to collate 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.**

---

[9] Report of the 2021 OEWG, A/75/816, Annex I, para 38.

E. Confidence-Building Measures

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

   a) The OEWG could agree to establish a global 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 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 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.

   b) Recalling the recommendation of the previous OEWG,[10] States 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 UNIDIR Cyber Policy Portal could be an avenue for sharing such information.

   c) It was proposed that aspects of confidence-building could include stakeholder engagement such as cooperation with interested stakeholders, 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 be strengthened and include the sharing and dissemination of good 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 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.

---

[10] Report of the 2021 OEWG, A/75/816, Annex I, para 50.

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 global points of contact directory as well as related initiatives for capacity-building and the sharing of best practices, and (b) the sharing of regional and sub-regional experiences 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 best practices on the operationalization of a global points of contact directory, which could include experiences at the regional level, and produce a report with options for the development of such a global directory 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 responses to either (a) the National Survey of Implementation, and/or (b) 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 and circulate all submitted information to delegations for discussion at the fourth session.

6. The OEWG Chair is requested to convene an inter-sessional meeting with States and interested stakeholders, including businesses, non-governmental organisations and academia, no later than the beginning of the fourth session, to explore the development and implementation of CBMs, 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 white papers, national strategies and policies including ICT capabilities as well as information on ICT institutions and structures, including through the UNIDIR Cyber Policy Portal.

F.   Capacity-Building

7.   States made concrete, action-oriented proposals on capacity-building. This non-exhaustive list of proposals may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a)   The OEWG could promote better understanding of the needs of developing States, for instance through encouraging participation in 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.

b)   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 in ICTs.

c)   States could consider establishing a permanent mechanism for exchanging views and ideas related to capacity-building in ICTs while taking into account existing initiatives. It was proposed that such a mechanism could be established within the UN.

d)   States could consider further funding for ICT capacity-building 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.

e)   States could strengthen coordination and cooperation between States and interested stakeholders, 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, (b) a permanent mechanism, potentially within the UN, for exchanging views and ideas related to capacity-building in ICTs while taking into account existing initiatives, 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.

3. **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.**

4. **The UN Secretariat is requested to designate an ICT capacity-building focal point with the responsibility of coordinating offers and requests for capacity-building, taking into account the proposals in paragraphs 7(a)-(e). The focal point could also coordinate capacity-building efforts by working 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 with interested stakeholders, including businesses, non-governmental organizations and academia.**

7. **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, and to collate information on these offers and share the information on the OEWG website.**

G.   Regular Institutional Dialogue

8. States made concrete, action-oriented proposals on regular institutional dialogue. This non-exhaustive list of proposals 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.

b) 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.[11] It was proposed that the PoA could be a mechanism to support capacity-building for

c) 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.**

2. **States engage in focused discussions on the elaboration of a PoA within the framework of the OEWG with a view towards its possible establishment as a mechanism to advance 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.**

.   .   .   .   .

---

[11] Report of the 2021 OEWG, A/75/816, Annex I, para 77.

Provisional Programme of Work[1]

Monday, 25 July

10 a.m.-1 p.m.   **Opening of the session**

Opening statements

- Ms. Izumi Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs

- H.E. Ambassador Burhan Gafoor, Chair of the Open-ended working group on security of and in the use of information and communications technologies 2021-2025

Agenda item 3: Organization of work

Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240

- Chair's presentation of the draft annual progress report

3-6 p.m.   **Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *(continued)*

First reading of, and negotiations on, draft annual progress report

- 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

- 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

---

[1] To be issued as document A/AC.292/2022/2

Tuesday, 26 July

10 a.m.-1 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *(continued)*

First reading of, and negotiations on, draft annual progress report *(continued)*

- How international law applies to the use of information and communications technologies by States

- Confidence-building measures

3-6 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *(continued)*

First reading of, and negotiations on, draft annual progress report *(continued)*

- Capacity-building

- Establish, under the auspices of the United Nations, regular, institutional dialogue with the broad participation of States

Wednesday, 27 July

10 a.m.-1 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *(continued)*

Thematic Discussion on Capacity-building

- Presentation by the United Nations Institute for Disarmament Research (UNIDIR) on best practices and lessons learnt with regard to international capacity-building efforts in UN disarmament processes (30 mins)

- Presentations by representatives of regional and subregional organizations on best practices and lessons learnt with regard to capacity-building efforts in the area information and communications technologies security (90 mins)

- Interactive exchange (60 mins)

3-6 p.m.	**Dedicated stakeholder session (in accordance with agreed modalities for the participation of stakeholders of 22 April 2022)**

- Interactive session with States and stakeholders on best practices and lessons learnt with regard to stakeholder involvement in capacity-building initiatives in the ICT security sphere (90 mins)

- Interactive session with States and stakeholders on how stakeholders can work with States to contribute to the implementation of the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report (90 mins)

Thursday, 28 July

10 a.m.-1 p.m.

Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 *(continued)*

Second reading of, and negotiations on, draft annual progress report

- 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

- 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

3-6 p.m.

Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 *(continued)*

Second reading of, and negotiations on, draft annual progress report

- How international law applies to the use of information and communications technologies by States

- Confidence-building measures

Friday, 29 July

10 a.m.-1 p.m.　　**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *(continued)*

Second reading of, and negotiations on, inputs to draft annual progress report

- Capacity-building

- Establish, under the auspices of the United Nations, regular, institutional dialogue with the broad participation of States

3 p.m.-6 p.m.　　**Agenda item 7: Adoption of annual progress reports**
- Adoption of first annual progress report

Agenda item 6: Other matters

Closing of the session

- Concluding remarks by the Chair

GUIDING QUESTIONS FOR DISCUSSIONS WITH STAKEHOLDERS AT THE THIRD SUBSTANTIVE SESSION

For discussion on best practices and lessons learnt with regard to stakeholder involvement in capacity-building initiatives in the ICT security sphere.

Suggested guiding questions:

1. What are the various ways in which stakeholders are currently involved in supporting and/or delivering capacity-building initiatives in the context of the current ICT security capacity-building landscape?

2. What kind of capacity-building initiatives or projects can stakeholders most meaningfully and effectively contribute to? Are there certain types of initiatives (e.g. technical training, skills training etc.) that present particularly suitable opportunities for meaningful and effective contributions from stakeholders?

3. What forms of stakeholder involvement (e.g. contribution of technical resources, co-creation of programmes, contribution of time and expertise of skilled individuals) work well and what forms of stakeholder involvement work less well?

For discussion on how stakeholders can work together with States to contribute to the implementation of the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG.

Suggested guiding questions:

1. With regard to the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report, are there any specific proposals which stakeholders can most meaningfully and effectively contribute to the implementation of, given their unique expertise, resources, knowledge and experiences. If so,

which proposals are these, and in what way can stakeholder holders contribute to their implementation?

2. With regard to the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG as captured in the draft annual progress report, are there any specific proposals which can be expanded to cover stakeholder groups? To consider one example, can a parallel Points of Contact directory be created by stakeholders to cover key contact points in the private-sector and technical community?

.   .   .   .   .

PERMANENT MISSION OF THE REPUBLIC OF SINGAPORE
UNITED NATIONS | NEW YORK

INVITATION

On the occasion of the third substantive session of the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025

H.E. Ambassador Burhan Gafoor,
Chair of the OEWG and
Permanent Representative of Singapore to the United Nations,

has the honour to invite the

Head of Delegation
plus one accompanying expert

to a Reception on
Monday, 25 July 2022, at 6.30 pm
at the
Permanent Mission of Singapore to the United Nations
318 East 48th Street
New York, NY 10017
(between 1st and 2nd Avenues)

To confirm your participation, please RSVP at https://bit.ly/oewg25july