Pre-draft of the OEWG's report on ICTs

GLOBAL PARTNERS DIGITAL

Global Partners Digital response

March 2020

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

GPD welcomes the Initial Pre-draft of the Open-ended Working Group (OEWG) report on ICTs and the opportunity to share our perspective on it.

Central to our input are two key points:

1. Discussions relating to peace and security in cyberspace—and what is permissible and impermissible behaviour in cyberspace—**are directly tied to and impact human rights**;
2. Due to the characteristics of ICTs as primarily civilian technologies, which were developed and continue to evolve due to the critical involvement of non-state actors, the maintenance of international peace and security in cyberspace **must be an effort inclusive of all stakeholders**.

In this response, we provide feedback on each of the sections in the descriptive part of the report—namely sections B-G. We also respond to each recommendation in section H, and where relevant suggest additional recommendations.

In our view, the pre-draft, while acknowledging the role of non-government stakeholders, **does not adequately refer to the varied and significant roles played by non-government stakeholders**, including civil society and the technical community, in promoting and protecting a peaceful and secure cyberspace. In addition, the report could further strengthen references and recommendations on promoting a human-centric and rights-based approach to a peaceful and secure cyberspace.

B. Existing and Potential Threats

GPD welcomes the pre-draft's acknowledgment of the differential impact of cyber threats (in paragraph 17). However, addressing the differential impact of cyber threats will require an approach inclusive of all relevant stakeholders**.** Therefore**, the report should further emphasise the role of different actors in addressing cyber threats**, and underscore the importance of taking special steps to involve stakeholders who are more vulnerable to cyber threats, including civil society organisations and marginalised communities.

Paragraph 16 refers to the differential capacity of states to deal with cyber threats. **It should also make clear that non-governmental actors, including civil society, have a role to play in addressing these differential capacities**—by highlighting the value they add in cyber capacity building efforts.

The importance of a human-centric and rights-based understanding, as mentioned in paragraph 12 of the narrative introduction, should be further emphasised. This section could highlight the need for states and other actors to continue discussions to identify the key elements and basis of a "human-centric lens" or understanding of threats, including by sharing their existing understandings of the term.

The report should also refer to the importance of a rights-based approach to addressing threats in cyberspace. For example, it refers to threats to "internal affairs of States through the use of ICTs, including by means of information operations and disinformation campaigns", "the exploitation of harmful hidden functions and the integrity of global ICT supply chains" and "the severity of threats to particular categories of critical infrastructure". Each of these threats directly impact a range of human rights, and—as such—should be addressed in a human-rights respecting and evidence-based manner. For example, **the human cost of attacks on critical infrastructure should be at the centre of understanding and responding to threats to critical infrastructure**. In addition, information gathering on the humanitarian and human rights impacts of intergovernmental operations should also be encouraged.

The report **should not refer to technological trends as threats in and of themselves**. Instead, **the report should recommend that measures to deal with malicious use of ICTs are human-rights respecting**, and that malicious use of ICTs by both non-state and state actors should not be used to justify measures which undermine human rights.

C. International Law

GPD welcomes the reaffirmation that international law—particularly the UN Charter—is applicable and essential to maintaining peace and stability (paragraph 22). **Human rights considerations should be considered a priority for states** as they engage in discussions at the First Committee on how international law applies to the use of ICTs. This is because international security and human rights are not mutually exclusive, but instead mutually reinforcing concepts. Respecting human rights and fundamental freedoms is essential for international stability, as it helps address underlying conditions that lead to global insecurity, and supports conditions favourable to human security.

GPD welcomes **the report's acknowledgment of international law as a foundation for stability and predictability,** and its emphasis on international humanitarian law as a means of discouraging militarisation and conflict.

Equally welcome is the OEWG's emphasis on enabling an interactive exchange of views by states on the relevance and applicability of specific bodies of law to the international security dimension of ICTs—including international humanitarian law, international human rights law, international criminal law, and international customary law (paragraph 24). **GPD believes strongly in the relevance and applicability of all these bodies of law to cyberspace**.

International human rights law, international humanitarian law, and international criminal law are foundational parts of the normative framework, and together create a complementary system for the protection of human rights, human life and justice. They further provide a structure through which state power is subject to agreed limitations that help foster international peace and stability.

We therefore support the view (captured in paragraph 24) **that these bodies of international law, complemented by the Group of Governmental Experts (GGE) norms, are currently sufficient for addressing state use of ICTs**. Efforts should be directed towards reaching a common understanding on how the existing normative framework applies and can be operationalised. States should carefully examine how all relevant branches of international law, including their respective instruments and principles, may be adapted to the use of ICTs. The voluntary norms are non-binding on states, but they represent consensus among states and directly reference Human Rights Council resolutions on human rights and ICTs. Over time, these voluntary norms, if widely adopted, may be reflected in state practice and *opinio juris,* which will ultimately provide clarity on how international law applies to state use of ICTs. States should keep these norms in mind as they develop their own national interpretations, and be encouraged to share these views publicly. **This should be emphasised in the OEWG's report**.

Two ways have been proposed to facilitate this exchange of views on international law: utilising the annual report of the Secretary General on developments in the field of ICTs in the context of international security, and the creation of a global repository (paragraph 30). **We support either of these non-binding initiatives as a way to involve all states**, many of which are currently unable to meaningfully engage, or have yet to produce their own interpretations. We also agree with the potential development of guidance notes (paragraph 31) on how existing international law applies to the use of ICTs, taking into consideration the specific characteristics of the ICT domain. However, further details are needed to ensure that existing human rights obligations would be adequately considered in the development of these guidance notes.

We disagree that a legally binding instrument (paragraph 28) is currently needed to address the unique characteristics of ICTs or the quickly evolving threat environment. International law has adapted to new phenomena in the past—such as international terrorism—without the need to create an entirely novel framework. States have already begun to publish their views on how international law applies to particular uses of ICTs, and the international community is now beginning to grapple with many unanswered questions. This ongoing process provides all states with an opportunity to engage and more avenues for other relevant actors to participate in these discussions. Moreover, there is no guarantee that a new binding instrument would lead to more effective global implementation of existing commitments or a stronger basis for holding actors accountable. This is because a new binding instrument may not explicitly reference existing commitments or require adequate protections for human rights. Technical advances made in recent years have also raised the prospect of more effectively attributing malicious activities and ensuring transparency in the absence of new mechanisms.

The international community should first acknowledge the ways in which the existing legal framework can already address the risks that state use of ICTs poses to international peace and security. For example, **we are encouraged that discussions called for a greater focus on key Charter principles such as the settlement of disputes by peaceful means** (paragraph 32). We welcome that some states "recalled existing mechanisms for the settlement of disputes, including the Security Council and International Court of Justice" and agree that these existing mechanisms should be prioritised by states as the primary means of seeking legal recourse for internationally wrongful acts. We recognise that the international community may eventually need binding commitments, but are unconvinced that they are necessary at the present moment. In the event that further commitments were needed, it would be imperative to first consider a politically binding commitment with regular meetings inclusive of all stakeholders, periodic reporting, and a clear priority for human rights.

D. Rules, Norms and Principles for Responsible State Behaviour

GPD agrees that "voluntary, non-binding norms of responsible State behaviour are consistent with international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights" (paragraph 34). GPD also believes that norms play an important role in preventing conflict.

We agree that there is a need to promote awareness of the existing norms and support their operationalisation (paragraph 37). However, **we recommend that the OEWG report should further emphasise the importance of operationalising the 11 voluntary and non-binding norms adopted by the General Assembly in 2015** (A/RES/70/237)—and that it **explicitly recognises the role of non-government stakeholders in supporting the implementation of these norms.** This includes their role in raising awareness and socialising the norms, capacity building, monitoring implementation, providing evidence-based research, and proposing specific technical and policy solutions to implement the norms. The report should also encourage states, in consultation with other stakeholders, to identify the relevant frameworks, including national cybersecurity strategies and policies, where the norms can be operationalised at the national and regional levels.

GPD agrees that gender perspectives should be mainstreamed into norm implementation (paragraph 34), and recommends that this is further broadened to include all human rights. As such, the report should highlight the importance and relevance of human rights in the implementation of the 11 norms. In GPD's submission to the "Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia" on 2-4 December 2019, we outlined the links between human rights and each of the 11 norms.

GPD agrees that further discussion and elaboration of new norms may be necessary (paragraph 38). However, for now, GPD believes that **the focus should be on implementation of the existing norms**. The development of any new norms should be done in a manner inclusive of all stakeholders and make reference to existing multistakeholder efforts, such as the work of the Global Commission on the Stability of Cyberspace in order to promote consistency and build on existing efforts.

GPD also believes that states should draw attention to acts contrary to the norms in order to increase accountability, transparency and help build habits of responsible behaviour. Creating transparent information-sharing mechanisms that are inclusive of all stakeholders is paramount to this, and relevant recommendations to this end are included in the last section.

We would also emphasise that efforts to operationalise norms exist around the world and should be recognised in the report. Multistakeholder efforts by the Internet Governance Forum (IGF)'s Best Practice Forum and the Global Forum on Cyber Expertise (GFCE) should be consulted, and the report should encourage member states to examine, capture, and build upon these efforts.

E. Confidence-building Measures

GPD agrees that a range of actors, including the private sector, academia and civil society have a role in contributing to building trust and confidence in the use of ICTs at national, regional and global levels (paragraph 47). However, we believe **the report could go further in outlining the role of non-governmental actors, including civil society, in operationalising and supporting implementation of regional and global confidence-building measures (CBMs) by states**.

For example, the CBMs developed in the 2015 GGE report on "advancing responsible State behaviour in cyberspace in the context of international security" focus on transparency and cooperation measures, such as facilitating "cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders" (A/70/174*)*. Such processes and mechanisms require wide stakeholder input; for example, the vast majority of commercial applications today use some open source components, which have been developed by a range of actors. As such, the addressing of threats and vulnerabilities through cross-border coordination will necessitate multistakeholder engagement.

Another CBM included in the 2015 report refers to the setting up of computer emergency response teams (CSIRTs). A number of multistakeholder initiatives, including those of the GFCE, provide best practice guidance in setting up CSIRTs. Non-state actors also play an important role in designing and facilitating table-top and scenario exercises to build capacity and trust among different stakeholders.

The report should further highlight the need for greater transparency around the adoption of CBMs at the national, regional and global levels and the involvement of non-state actors in monitoring their implementation and measuring their effectiveness.

F. Capacity-building

GPD agrees that capacity building plays a critical function in empowering all states and other relevant actors to fully participate in the global normative framework (paragraph 48).

However, GPD believes **that the report shold also refer to the importance of holistic capacity building**, whereby capacity building is understood to encompass a wide range of efforts, including the development of cybersecurity policy, cyber incident management and critical infrastructure protection, cybercrime, cybersecurity culture and skills and cybersecurity standards.

GPD agrees that attention should be given to addressing the "gender digital divide" (paragraph 56). **The report should go further in underlining the importance of rights-based and inclusive approaches to all capacity building efforts**. This means that civil society should be engaged in both the development and implementation of capacity building efforts. Our submission to the December 2019 OEWG intersessional meeting sets out the links between human rights and cyber capacity building.

GPD's recommendations on cybersecurity capacity building principles are included in our response to section H below.

G. Regular Institutional Dialogue

GPD agrees with the report that **any platform for regular institutional dialogue should build on previous agreements, and be inclusive, consensus-driven, sustainable, and results-oriented**, with specific objectives that take forward agreements in practical and tangible ways (paragraph 59). We also think the report should emphasise that all stakeholder groups have a role to play in both formulating and implementing recommendations and measures developed to promote ICT security in the context of international peace and security.

Therefore, **the report should explicitly mention the importance of institutional dialogue that is meaningfully inclusive of all relevant stakeholders, including civil society**. Further, it should note that financial resources to engage are essential, particularly for stakeholders in the global South and civil society groups.

GPD recognises that there are established venues within the UN Disarmament Machinery where ICTs and international security could be addressed using existing resources, including the General Assembly's First Committee and the United Nations Disarmament Commission, as well as external venues (paragraph 60). GPD also recognises that there may be value in considering the option of continued regular dialogue under UN auspices through the renewal of the OEWG's mandate. However, **it is crucial that discussions around the potential continuation of the OEWG include meaningful consultation with all relevant stakeholders, including non-ECOSOC accredited NGOs**. This premise should also underpin the potential modalities for a renewed OEWG.

GPD also agrees on the need for greater exchange and exploration of synergies between established forums within the UN system focused on issues related to ICTs (paragraph 61). At the same time, discussions relating to ICTs and the responsible behaviour of stakeholders aren't exclusive to the UN system, but are increasingly taking place at the national and regional levels, as well as in other global forums. **The report should therefore call for greater exchange and exploration of synergies between relevant forums and processes, both within and outside the UN, in order to ensure discussions are complementary.**

H. Conclusions and Recommendations

a) With regard to international law, reaffirming that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment, the OEWG recommends that:

- Member States be invited to continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information about national views and practice on how international law applies to State use of ICTs in the context of international security.

Recommendation: We agree that states should be invited to continue to inform the Secretary-General of their views and to include additional information about national views and practice. We additionally recommend that states specifically include their views on how human rights and fundamental freedoms apply in this context. Moreover, states should prioritise international human rights considerations, because international security and human rights are mutually reinforcing concepts. It is imperative that human rights considerations are taken into account by states as they develop national views, as this will help address the underlying conditions that lead to global insecurity.

Recommendation: International peace and security rests on various bodies of international law, including international human rights law, international humanitarian law, and international criminal law. States should carefully examine how all relevant branches of international law, including their respective instruments and principles, may be relevant or adapted to state use of ICTs.

- Member States be invited to submit, on a voluntary basis, national views and practice on how international law applies to State use ICTs to the Cyber Policy Portal of the United Nations Institute for Disarmament Research.

Recommendation: We support the voluntary submission of national views and practice to the Cyber Policy Portal of the United Nations Institute for Disarmament Research. These voluntary submissions would provide all states with an opportunity to advocate for human rights considerations in an open manner, and establish an inclusive mechanism to address varying interpretations on how international law applies to state use of ICTs.

- The Secretary-General be requested to establish a repository of national views and practice on how international law applies to the use of ICTs by States in the context of international security.

Recommendation: We support the establishment of a repository of national views and practice on how international law applies to the use of ICTs by states in the context of international security. As noted in the previous recommendation, this approach would help states reach a common understanding on how the already agreed upon normative framework applies and can be operationalised, particularly with regard to existing international human rights obligations. It also provides states that have not been active in these discussions with an opportunity to meaningfully engage and share their views.

- The International Law Commission be requested by the General Assembly to undertake a study of national views and practice on how international law applies in the use of ICTs by States in the context of international security.

Recommendation: We support a request by the General Assembly for the International Law Commission (ILC) to undertake a study of national views and practice on how international law applies in the use of ICTs by states in the context of international security. The ILC has played an essential role in developing and codifying international law in the past due to its objectivity and impartiality, which could be replicated in this particular circumstance. Accordingly, states should be encouraged to develop and publish their national interpretations of how international law applies to state use of ICTs in order to assist the ILC.

- *[other recommendations]*

Recommendation: We strongly advise against the development of a legally binding instrument to address the unique characteristics of ICTs or the quickly evolving threat environment at this time. States should instead consider the ways in which the existing legal framework can already address the risks that state use of ICTs poses to international peace and security. Particular attention should be made on adherence to key Charter principles, such as the settlement of disputes by peaceful means, and respect for human rights and fundamental freedoms.

Recommendation: States should use existing mechanisms, particularly the Security Council and International Court of Justice, when seeking legal recourse for disputes that arise through state use of ICTs. These mechanisms are most likely to result in peaceful settlement of disputes and facilitate common understanding of unresolved questions that arise in the existing international legal framework.

- Member States continue to consider, at the multilateral level, how international law applies in the use of ICTs by States in the context of international security.

Recommendation: We support state efforts to consider how international law applies to the use of ICTs in the context of international security at the multilateral level. While the primary focus of states should be the development of national interpretations on how international law applies, existing multilateral forums and mechanisms provide an essential means of reaching a common understanding on key issues. In addition, states should also consider and engage in these discussions in multistakeholder forums. Discussions at both the multilateral and multistakeholder level should be inclusive and prioritise respect for human rights and fundamental freedoms in both international and regional forums.

b) With regard to rules, norms and principles of responsible behaviour of States, reiterating that voluntary, non-binding norms are consistent with international law, and recalling that in 2015 the General Assembly agreed by consensus that all States should be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts, which sets out 11 voluntary, non-binding norms of responsible State behaviour, the OEWG recommends that:

- Member States be invited to continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information on their implementation of international rules, norms and principles of responsible behaviour of States in the use of ICTs.

Recommendation: We agree that member states should continue to inform the Secretary-General of their views and assessments, and to include additional information on their implementation of rules, norms and principles. We suggest that this recommendation should go further by recommending that states consult with other stakeholders, including civil society, in the development of their views and assessments.

- The Secretary-General be requested to establish a repository of national practices regarding international rules, norms and principles of responsible behaviour of States, which could be further developed into guidance on implementation. The use of surveys or templates on a voluntary basis are encouraged in this regard.

Recommendation: GPD believes that the establishment of a repository of national practices regarding international rules, norms and principles, based on surveys or templates, would be useful. This should complement a mechanism which allows for the annual sharing of experience and practice by states of their implementation of international rules, norms and principles of responsible behaviour, in a way which is inclusive of all relevant stakeholders. It is important that any repository be transparent and publicly available—for example, via The United Nations Institute for Disarmament Research (UNIDIR)'s Cyber Policy Portal.

- Further guidance on the implementation of norms of responsible State behaviour be developed and widely disseminated at national, regional, interregional and global levels including through the United Nations. States in a position to contribute expertise or resources to the development and dissemination of such guidance are encouraged to do so.

Recommendation: GPD agrees that further guidance on the implementation of norms of responsible state behaviour be developed and disseminated. However, further details are needed to ensure that existing human rights obligations would be adequately considered in the development of this guidance. As noted above (page 4), both gender and broader human rights considerations should be mainstreamed into the implementation of norms. Non-governmental stakeholders should be consulted in the development of this guidance. The guidance should proceed on an evidence basis, informed by challenges which are being faced by states and other stakeholders in implementing the norms.

- [other recommendations]

Recommendation: The OEWG report should call for the establishment of an information sharing mechanism to support the implementation of the 11 GGE norms (Res 70/237), allow for the capturing of lessons learned, as well as increasing awareness of the norms, building trust and confidence, creating incentives for compliance and thereby ensuring the observation of norms. Assessments of norm implementation should be periodic and publicly available, and permit non-government stakeholders to participate.

Recommendation: The OEWG report should both recognise the need for and support multistakeholder, independent and coordinated attribution efforts.

Recommendation: The OEWG report should encourage states, in consultation with other stakeholders, to identify the relevant frameworks, including national cybersecurity strategies and policies, where rules, norms, and principles for responsible state behaviour can be operationalised at the national and regional levels.

Recommendation: The report should include reference to the need for states to commit to holding private sector actors to account, in line with the proposal by Croatia, Finland, France and Slovenia in the "non-paper— that "States take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory". However, this proposal should be strengthened by referring to the UN Guiding Principles on Business and Human Rights. In particular, it should refer to Principle 3(a): "In meeting their duty to protect, States should: (a) Enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps."

Recommendation: We support the recommendations by the Netherlands in the "non-paper", to elaborate on and provide further guidance on norms (f) and (g) in the UN GGE 2015 report (Res 70/237)—namely that "State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace"; and "State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites".

- Member States continue to consider, at the multilateral level, international rules, norms and principles of responsible behaviour of States.

Recommendation: GPD believes that member states should continue discussions of international rules, norms and principles of responsible behaviour of states in both multilateral and multistakeholder forums and processes. All intergovernmental initiatives, as well as multistakeholder initiatives, should be open, inclusive and transparent. In this way, stakeholders can bring to the table their own perspectives, evidence, research and proposals for solutions. This will help avoid duplication between efforts and will identify synergies.

c) With regard to confidence-building measures (CBMs), highlighting that CBMs should be developed and implemented progressively, including at the bilateral, regional and multilateral levels, so as to enhance mutual trust, the OEWG recommends that:

- The Secretary-General be requested to establish a repository of CBMs adopted at regional and sub-regional levels to enable the sharing or exchange of information on CBMs and identify potential capacity and resource gaps. The repository would be established in coordination with interested regional and sub-regional bodies and without prejudice to further elaboration of CBMs at the global, regional or sub-regional level.

Recommendation: GPD supports this recommendation, and would encourage the repository to be developed in consultation with non-government stakeholders, including civil society, in relevant regional and sub-regional bodies.

- Member States be encouraged to, on the basis of such a repository, potentially identify the CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.

Recommendation: GPD supports this recommendation, and suggests that the recommendation also refer to the need to cooperate with all other relevant stakeholders in their implementation.

- The Secretary-General be requested to establish, in coordination with interested regional and sub-regional bodies, a global registry of national Points of Contacts at the policy or diplomatic level, bearing in mind coordination with other such registries, including at the regional and sub-regional levels.

Recommendation: GPD supports this initiative, but recommends that the importance of designing and maintaining a global registry with security in mind are underscored.

- Member States, which have not yet done so, be encouraged to nominate a national Point of Contact at the policy or diplomatic level, taking into account differentiated capacities.

- Members States be encouraged to explore mechanisms for regular cross-regional exchanges of lessons and good practices, taking into account differences in regional contexts and the structures of relevant organizations.

Recommendation: GPD supports this recommendation and encourages leveraging existing coordination and information sharing platforms, including the GFCE.

- Member States continue to consider CBMs at the bilateral, regional and multilateral levels.

Recommendation: GPD believes that member states should consider CBMs in both multilateral and multistakeholder forums and processes. All intergovernmental initiatives, as well as multistakeholder initiatives, should be open, inclusive and transparent. In this way, stakeholders can bring to the table their own perspectives, evidence, research and proposals for solutions. This will help avoid duplication between efforts, and identify synergies.

d) With regard to capacity-building, emphasizing its critical functions for empowering all States and other relevant actors to fully participate in the global normative framework, for promoting adherence to international law and the implementation of norms of responsible State behaviour, and for building trust between and within States, the OEWG recommends that:

- ICT-related capacity-building efforts in the field of international security should be guided by the following principles:
    - [insert agreed principles]

Recommendation: We recommend that capacity building efforts should be underpinned by human rights and that relevant processes to develop and implement capacity building should be open, inclusive and transparent. This means that capacity building should be rights-based by design, with safeguards to protect fundamental rights and freedoms and support the engagement of civil society in the development and implementation of capacity building efforts. It also means that capacity building efforts should be developed and implemented through open, inclusive and transparent processes, facilitating the meaningful engagement of relevant stakeholders.

We further recommend that the report take note of the principles which underpin the GFCE, included below:

- *Inclusive partnerships and shared responsibility*: effective cyber capacity building requires cooperation across nations, including various stakeholders, and at different levels;
- *Ownership*: partner nations need to take ownership of capacity building priorities;
- *Sustainability:* obtaining sustainable impact should be the driving force for cyber capacity building;

- *Trust, transparency and accountability:* transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation.

We support the need for capacity building efforts to be “demand-driven, tailored to specific needs and contexts, evidence-based, results-oriented, and have sustainable impacts” and be “non-discriminatory, gender sensitive and focused on peaceful outcomes” (paragraph 52).

- Member States be invited to continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information on lessons learned and good practice related to capacity-building programmes and initiatives.

Recommendation: GPD supports this recommendation. However, we recommend that it is strengthened by referring to the importance of engaging non-government stakeholders, including civil society, in developing and sharing lessons learned and good practice related to capacity building programmes and initiatives.

- The Secretary-General be requested to establish a global mechanism for enhancing coherence in capacity-building efforts in the use of ICTs, possibly in the form of a facilitation mechanism, in coordination with existing efforts, including at the regional and sub-regional levels. States in a position to contribute expertise or resources to the development of such a mechanism are encouraged to do so.

Recommendation: GPD recognises the need for enhanced coherence in capacity building efforts. However, the OEWG should emphasise the importance of identifying existing initiatives and finding opportunities for collaboration with them, both within the UN (e.g. the Technology Facilitation Mechanism and the IGF) and outside the UN (e.g. GFCE). We would also recommend that the OEWG take stock of existing capacity building efforts and requirements, in order to both determine issues and topics where further capacity building expertise and processes be necessary and identify possible duplications of effort.

- Member States be encouraged to further cooperate to build capacity to identify and protect national and transnational critical infrastructure as well as supranational critical information infrastructure.

Recommendation: GPD supports this recommendation but believes it should be strengthened by referring to the need to ensure the human cost of attacks on critical infrastructure are at the centre of understanding and responding to threats to critical infrastructure. Further, it should emphasise the need to cooperate with all relevant stakeholders in building capacity to identify and protect national, transnational and supranational infrastructure.

- [other recommendations]

- Member States continue to consider capacity-building at the multilateral level.

Recommendation: GPD believes that member states should consider capacity building at both multilateral and multistakeholder forums and processes. All intergovernmental initiatives, as well as multistakeholder initiatives, should be open, inclusive and transparent.

In this way, stakeholders can bring to the table their own perspectives, evidence, research and proposals for solutions to the table. This will help avoid duplication between efforts and will identify synergies.

e) With regard to regular institutional dialogue, affirming that the increasing dependency on ICTs and the scope of threats stemming from their misuse necessitates urgent action to enhance common understandings and intensify cooperation through multilateral discussions, the OEWG recommends that:

- The 76th session of the General Assembly of the United Nations convene a new open-ended working group of the General Assembly acting on a consensus basis to continue the consideration of developments in the field of information and telecommunications in the context of international security.

Recommendation: GPD believes that the renewal of any dialogue under the auspices of the UN should ensure meaningful engagement of non-governmental actors, including civil society and NGOs which are not ECOSOC accredited. This should be strongly emphasised in the report. It should also be noted that financial resources to engage are essential, particularly for civil society groups and stakeholders from the global South.

- States be encouraged to consider establishing sponsorship programmes and other support mechanisms to ensure broad participation. States in a position to support such programmes and mechanisms are encouraged to do so.

Recommendation: We support this recommendation, suggesting that it also ensure that such sponsorship programmes are primarily aimed at underrepresented states and groups, such as women. In addition, the report should encourage states to provide support for the meaningful engagement of civil society, particularly from underrepresented countries and regions.

- The 76th Session of the General Assembly of the United Nations also consider requesting the Secretary-General to establish a new group of governmental experts.

Recommendation: The OEWG report should underscore the need for any dialogue to ensure meaningfully open, inclusive and transparent engagement of non-governmental stakeholders. This could include the development of open, inclusive and transparent national and regional consultation mechanisms, to ensure consultation and exchange mechanisms with respective civil society and other stakeholder groups.

- *[other recommendations]*

Recommendation: The OEWG report should request that member states also take note of the report of the “Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019)”.