DiploFoundation is pleased to further support the work of the OEWG 2021–2025 by offering knowledge in the form of direct contributions and providing capacity-building programmes to strengthen the participation of developing countries in this important process.

As a supporter of and contributor to the OEWG since 2019, DiploFoundation is deeply concerned by some OEWG member states recently using their veto to exclude a large number of relevant actors from contributing to the future process. This decision goes directly against the established framework of responsible behaviour, in particular the agreements of the GGE and OEWG in 2021, which unequivocally confirm the important role that all stakeholders play in shaping and implementing the norms and principles of responsible behaviour. In times of increased geopolitical tension, dialogue is needed more than ever. For this, we need all the knowledge, capabilities, and skills available to support the OEWG in its important mission. Therefore, we urge UN member states participating in the OEWG to reconsider their decision and apply their right of veto responsibly, proportionally, transparently, and in good spirit, for the benefit of the successful work of the OEWG.

In response to the invitation by the Chair of the OEWG dated 22 June 2022 to interested, non-governmental stakeholders to share their views on the topics under consideration by the OEWG, and in particular, on the Zero-Draft report and the guiding questions for discussion with stakeholders, DiploFoundation hereby provides our contribution to the third substantive session of the OEWG.
The following contribution provides:

1) Reflections on the proposed Zero-Draft report.
2) Responses to the guiding questions for discussion with stakeholders.

For additional context on contributions related to capacity-building based on our cyber capacity-building work since 2002, please refer to the submission of DiploFoundation to the OEWG of April 2020, available at the OEWG website or directly at:


DiploFoundation remains available for additional inputs, as well as for new partnerships in this field.

1) Reflections on the proposed Zero-Draft report

B. Existing and potential threats

Exploiting vulnerabilities remains one of the key threats in cyberspace. Yet, it is not sufficiently recognised as such by the OEWG.

Within ‘Technical and cooperative measures to address existing and potential threats’, as well as recommendations related to ‘States utilizing the framework of the OEWG to further exchange technical information relating to existing and potential threats’, it is necessary to include a direct reference to cooperation on enhancing vulnerability disclosure and treatment practices and policies, and preventing the exploitation of vulnerabilities.

For additional context on addressing the threats from vulnerability exploitation in the context of the OEWG’s work, refer to the submission of DiploFoundation to the OEWG of 10 December 2021, available at the OEWG website or directly at:


C. Rules, norms, and principles of responsible state behaviour

In the context of the implementation of norms under the existing framework of responsible behaviour, it is important to also observe the roles of non-state stakeholders and ensure the involvement of their knowledge, skills, and capabilities in implementing the norms.

Recommendations should, therefore, encourage interested states or groups of states that are invited to submit working papers to consult with other relevant stakeholders on national, regional, and global levels – in particular (but not limited to) with regard to developing a common understanding of technical information and communication technology (ICT) terms.

E. Confidence-building measures
The initiative to establish a directory of global points of contact on ICTs at the UN, which is gaining momentum, is of extreme importance for the timely reaction to incidents with wider geographical, political, social, and economic impact. In establishing this directory – and a possible future network – the OEWG can benefit from the vast experience of the technical community, the private sector, and civil society in this field. Involving these players in the contact directory would be of particular relevance in relation to vulnerability treatment, early warnings about critical cyber incidents, and information sharing and cooperation.

In this regard, the proposal that ‘Points of Contact in the private sector could be established as appropriate’ can be extended to ‘Points of Contact with other relevant actors from the technical community, civil society, and academia’. In recommendations, the UN Secretariat, which ‘is requested to collate best practices on the operationalization of a global points of contact directory, which could include experiences at the regional level’ should also collect experiences from the private sector, technical community, civil society, and academia.

F. Capacity-building

The OEWG initiative to play a role in encouraging cooperation between online portals and compiling a calendar and ‘offers’ of capacity-building programmes and a list of implementing organisations (rather than only ‘centres of excellence’) is also of great relevance. In this regard, it is important that the OEWG does not duplicate the role of any existing regional and global capacity-building mechanisms and programmes, but rather enhances their outreach and assists with better coordination of donors and implementers.

In addition, as cyber issues crosscut other thematic areas that may impact international peace and security as well (such as cybercrime, health, energy, space, and lethal autonomous weapons systems) there is a need to enhance the mapping of other relevant capacity-building initiatives in these fields. This would ensure a holistic approach to capacity-building and the cross-pollination of knowledge and experience across thematic and organisational silos.

In the recommendations, states should not necessarily engage in solely ‘funding ICT capacity-building through [...] integration with larger development programmes’ (since large programmes bring large operational costs as well, and this approach carries a risk of reducing funding for important niche topics or local and emerging programmes), but should rather emphasise better coordination of donors, as well as various implementing organisations (to avoid duplication and address the right gaps). In this regard, the proposed establishment of an ICT capacity-building focal point to enhance coordination is commended; the focal point could ensure the mapping of a broader set of capacity-building initiatives in other thematic fields that have cyber components and impact international peace and security.
2) Responses to the guiding questions for discussion with stakeholders

In response to the Chair’s guiding questions on best practices and lessons learnt with regard to stakeholder involvement in capacity-building initiatives in the ICT security sphere, DiploFoundation will use this contribution to highlight the relevant key areas in capacity-building.

Question 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?

The technical community, private sector, and civil society organisations have a deep understanding of how cyberspace and its actors operate and evolve, and of existing and potential threats. They are often the ones to implement cybersecurity measures and increase the awareness of other actors. There exists a great number of capacity-building initiatives by states, the private sector, academia, and foundations that provide expertise and resources.

The initial step is therefore for all the states (as well as regions and sub-regions) to have the capacity to assess their needs related to their ICT security and identify gaps that need to be addressed. As of now, the ability of states to do so differs widely. Once the states can identify their needs, existing capacity-building initiatives can be matched and new ones developed. This should be conceived as a continuous process to reflect the developing and emerging needs of states and the ICT security landscape.

DiploFoundation’s work for the past 20 years has focused on one aspect of such capacity development: strengthening the cybersecurity policy and cyber diplomacy capabilities of states, especially small and developing ones, to participate in relevant international negotiations on a more equal footing. We would be honoured to share additional information on the non-partial capacity-building programmes DiploFoundation provides.

Question 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) that present particularly suitable opportunities for meaningful and effective contributions from stakeholders?

Speaking from our 20 years of experience, any meaningful and effective capacity-building initiatives, whether contributed by stakeholders or the states themselves, need to fulfil certain attributes.

Sustainable capacity-building outcomes can only be achieved by long-term and continuous capacity-building programmes. These need to address the specific needs of states in a neutral manner.

As the issues of ICT security affect different areas, capacity-building needs to be multidisciplinary to address cross-cutting issues. A balanced, holistic approach to capacity-building delivers the most
effective and lasting outcomes. While technical skills are often mentioned, there is an increasing need for building individual and institutional capacity in a range of diplomatic, policy, legislative, and regulatory areas. Equally important is connecting security perspectives with a broad view of regulatory and policy issues, in particular relating to economic development and human rights. Since cyber cuts across various non-cyber thematic areas – such as disarmament, economic supply chain, energy security, and security in the context of sustainable development – holistic capacity-building needs to connect those silos as well.

ICT security is global, regional, national, and local. Effective capacity-building must reflect this and provide for integrated efforts to build up the ability of states in the ICT security area on all levels. Of particular relevance are cross-border capacity cooperation and the exchange of experiences, challenges, and good practices. Therefore, capacity-building programmes on regional or even global levels are particularly relevant and within reach, especially by walking the talk and utilising interactive online learning and knowledge exchange approaches.

**Question 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?**

The involvement of various stakeholders in the OEWG process contributes to more informed decision-making by states and assists states to clarify their positions within the OEWG, thus aiding the negotiation and outcomes of the process.

Limitations on stakeholder participation or limitations of topics on which the stakeholders can provide their inputs could result in incomplete and unbalanced information being available to states and, in some cases, their ability to negotiate effectively for their aims. This particularly impacts small and developing states, as well as those with the greatest need for capacity development in ICT security.

The particular forms of stakeholder involvement shall be determined by the states themselves and tailored to their specific needs. Ideally, states should not only welcome full consultative involvement of other stakeholders in the OEWG but also increase consultations with and involvement of stakeholders in shaping their own national policies and positions taken at the OEWG.

We reiterate that politically neutral, comprehensive, inclusive, and transparent capacity-building is of the utmost urgency and importance.