**Observations from the European Union on the draft guidelines for utilisation of the Global Cybersecurity Agenda of the ITU.**

**Pillar 1: Legal measures, point 2.9 of the draft guidelines:**

*“a. ITU should continue its efforts to facilitate multi-stakeholder discussions and collaboration on the challenges associated with addressing the issue of cybersecurity, and in particular strengthen its relationship with partners and other stakeholders to deliver assistance to Member States in this regard.*

*b. ITU should continue to work with partners to develop and maintain resources, such as the Cybercrime Legislation Resources, to help Member States understand the legal aspects of cybersecurity, while also exploring opportunities to work with Member States to support development of frameworks on the subject, including legislation, if so requested.*

*c. Member States are urged to design and develop any appropriate legal measures in accordance with their fundamental human rights obligations.*

*d. Member States are encouraged to cooperate as well as work together with other stakeholders to search for a global common ground on legal measures on cybersecurity, while noting and modelling existing frameworks such as the Council of Europe Convention on Cybercrime of 2001:*

Observations:

* In general, the recommendations in this section of the guidelines pose questions with respect to the remit of the ITU in some aspects given that there are relevant discussions in the UNGA, Council of Europe and elsewhere. In particular, issues related to criminal justice do not fall under the remit of the ITU.
* The draft guidelines suggest that the Council of Europe Convention on cybercrime (the Budapest Convention) might be outdated and encourages Member States ‘to search for a global common ground on legal measures on cybersecurity, while noting and modelling existing frameworks such as the Council of Europe Convention on Cybercrime of 2001’.
* The Budapest Convention is the best model for countries seeking to develop their own national legislative approach.  It is a comprehensive multilateral legal framework that allows for increasing international capacity and cooperation.
* The Budapest Convention provides a strong model, which we consider as an effective standard of cyber legislation also in the context of emerging digital technologies such as those enumerated in the report. The Convention is technology-neutral so that the substantive criminal law offences may be applied to both current and future technologies involved, while its overseeing Cybercrime Convention Committee is mandated to issue Guidance Notes to facilitate the effective use and implementation of the Convention, also in the light of legal, policy and technological developments. The second additional Protocol which is currently negotiated also aims at addressing remaining challenges by opening new channels of international cooperation.

**Pillar 2: Technical and procedural matters, Point 3.12 in the context of elaborations in point 3.9:**

*“a. All recommendations made in the HLEG Report 2008 (Recommendations 2.1 – 2.16) are still valid. All Member States are encouraged to commit to a shared global cybersecurity vision, to continue to implement these recommendations (2.1 – 2.16), and to support ITU in becoming “the global centre of excellence” for developing Recommendations on technical and procedural measures for cybersecurity in areas within its mandate (as referenced in the HLEG Report 2008).*

*b. ITU study groups should focus on emerging security technologies in order to study and formulate guidelines for the use of related technologies, and guide Member States on applying these in a timely manner in order to counter changing and escalating cyber threats.*

*c. A mechanism for close cooperation should be established among the various ITU-T study groups regarding the study of security-related matters, with SG17 in a coordinating/leading role, so that the highest possible degree of end-to-end security is maintained throughout the standardization process of all components and interfaces of ICT products.”*

Observations:

* While the recommendations above address the work of ITU standardisation sector (ITU-T), the reference to development of “norms” in the draft document could be interpreted as referring to the development of norms to guide responsible State behaviour in their use of ICTs. This point should be further clarified in the text.
* In this context, it is worth recalling that the EU and its Member States do not believe that it is appropriate to support the ITU in becoming the “global centre of excellence” for development of such norms. The EU and its Member States strongly support existing efforts regarding the application of existing international law; the development and implementation of universal norms of responsible State behaviour; and regional confidence building measures between States within the UN framework, in particular the UN GGE and OEWG.

**Pillar 5: International cooperation, point 6.17:**

*“a. The United Nations has a unique role in fostering cooperation, dialogue, and coordination among all nations, as well as with the private sector and other stakeholders, on global cybersecurity matters. ITU, considering its position in the UN system as the specialized agency for ICTs, and sole facilitator of Action Line C5 (Building confidence and security in the use of ICTs) should continue to play a leading role, within its mandate, in related developments.”*

*“b. Based on the WSIS Process and taking into account the efforts of the UN Secretary-General’s High Level Panel on Digital Cooperation – especially Recommendation 4 (Global Commitment on Trust and Security), ITU should help strengthen facilitation efforts in bringing different players together, including the conveners of the various processes. These could be through the mechanisms offered under Action Line C5 related processes through the WSIS Forum, as well as those offered by the IGF, among others.”*

*“c. While bilateral and multilateral discussions among key players should continue to be encouraged, given the global nature of cyber threats, it is also important that broader discussions should be facilitated among wider groups, including the private sector and other stakeholders. ITU could play a key facilitating role in this regard – working with partners to help bring together Member States and other stakeholders within the wider global context of the United Nations.”*

Observations:

* The EU and its Member States support the ITU existing role under agreed resolutions in promoting international and multi-stakeholder cooperation, confidence and security in the use of ICTs and capacity building.
* We welcome ITU involvement to support broader discussions among wider group of stakeholders in particular through the WSIS process and encourage the ITU to foster such multi-stakeholder dialogues to help strengthening existing multi-stakeholder dialogues within the UN, as well as other processes, such IGF and initiatives including the private sector.
* Moreover, ITU’s Child Online Protection platform providers a successful model for multi-stakeholder cooperation and should be further promoted.
* While the ITU plays a valuable role in convening a multi-stakeholder discussion under the WSIS processes, important discussion is ongoing within existing framework, notably in the UN, First Committee, as well as Digital cooperation initiative of the UNSG under the work stream Trust and Security in cyberspace.
* In this context, recommendation that could undermine or either pre-empt the outcomes of these initiatives should be avoided. We do not see a leading role of the ITU for a global cybersecurity framework.

**General conclusion of the draft guidelines for the GCA Framework:**

*(c)“ITU should serve as a repository of information for the various global activities, initiatives, and projects that are being carried out on different facets of cybersecurity by other stakeholders and organizations active in this field, and who may have the lead mandate, role and/or responsibilities in those specific facets, in order to enable the international community to have an easy point of access to all such resources.”*

*(e) ITU should continue to follow the development and use of new and emerging ICTs in order to guide Member States and stakeholders on the security aspects of these technologies and, where relevant, their potential application to counter cyber threats.*

Observations:

* Recalling the ongoing work within the UN framework, namely the OEWG and the UN GGE, the EU and its Member States are of the view of building upon existing and agreed work and would further promote synergies before creating an additional platform, such as the global repository.
* Moreover any new repository at the ITU could create duplication of work with other fora and put a considerable burden on the limited resources of the ITU (in terms of updating, maintenance etc).
* Regarding the recommendation (e), as recognized by previous UN GGE reports, given the unique character of ICT technologies, our approach must remain technology neutral. This is consistent with the concept and UN acknowledgement that existing international law applies to new areas, including the use of emerging technologies. Therefore, the EU and its Member States recognize that the ongoing discussion within the First Committee of the UNGA provide a good platform to the whole UN membership to engage on the malicious use of emerging technologies in the context of international peace and security, and further address the responsible State behaviour in their use of ICTs.