France’s response to the pre-draft report from the OEWG Chair

As the international community faces a major health crisis, the critical nature of healthcare infrastructures and the importance of information technologies to maintain social cohesion and to continue certain essential economic activities are receiving renewed attention. The realization of our dependence on these tools also highlights how topical and important the discussions at the OEWG are to protect our societies.

France commends the work of synthesis and coherence conducted by the Chair and its supporting teams. France would like to highlight the following considerations in view of the second draft of the report.

1. General points

France welcomes the general content of the report and the balanced presentation of the different positions. As is currently the case in the pre-draft, it seems particularly important to ensure the report from the OEWG is in line with the work previously conducted and agreed at the UN, including the results of the five previous GGEs, and to reaffirm the complementarity of the OEWG and the ongoing GGE. France considers it necessary for the report to recognize the acquis of the previous working groups.

France would like greater weight to be given to highlighting the final ambition of the work carried out at the UN and in the OEWG: preserving international security and peace and preventing conflicts. These points are worth being presented more clearly and systematically from the introduction onwards and throughout the text, including the commitment of States to live together in peace with one another as good neighbours, as they are bound to do so by the Charter of the United Nations.

Similarly, the information in paragraph 10, which aims to highlight how information technology issues are interconnected and influence other areas of the work of the United Nations - peace and security, human rights and sustainable development-could come earlier in the text.

Lastly, the report could be more explicit about the link between threat assessment, international law, norms, capacity building and confidence-building measures. Taken individually, none of the parts of the report should allow divergences in interpretation concerning the commitments of States or the value of agreed principles. The importance of norms is expressed in various ways throughout the text, which is something worth harmonizing, particularly to reaffirm that the norms agreed within the United Nations, including those agreed during GGE sessions, are binding on States and are not just mere “guidelines”.

II. Existing and Potential Threats

Several points attracted our attention within the Existing and Potential Threats section.
Concerning paragraph 15, France would like to qualify the elements in the draft reports on the militarization of cyber space. The acquisition and the development of cybernetic capacities contribute to guaranteeing the sovereignty of States and could not contravene to the peaceful use of cyberspace so long as there use are conditioned to the respect of International Law, especially to the Charter of the UN. The issue of interference and disinformation operations mentioned in the same paragraph, while not directly linked to the group’s mandate, is a particularly concerning threat. If the subject has to appear in the report, relevant fora handling these issues could be mentioned, in order to promote and encourage the work currently underway in these areas at the UN. It is also necessary to acknowledge that not all disinformation campaigns should be considered as a breach of the principle of non-intervention, since such a qualification is to be based on two cumulative conditions: a violation of the domestic jurisdiction of the State and the use of constraint.

In paragraph 18, the inherently neutral nature of technologies, which was highlighted in session, is mentioned. It is essential that it remains in the final report, and it could perhaps be mentioned in the introduction.

In paragraph 19, the points concerning the importance and specific nature of threats against regional or transnational critical infrastructure are particularly relevant and could be the subject of further developments insofar as they involve particular challenges. More space could be dedicated to field of vital importance such as healthcare, finance, transport, and electoral infrastructures. A more particular emphasis could be laid on healthcare infrastructures whose importance to our societies is once again being underlined by the current pandemic.

III. International Law

France would like to reaffirm the full applicability of international law in cyber space, including the Charter of the United Nations and international humanitarian law. Whereas the applicability of international law was affirmed in the 2013 and 2015 reports adopted by consensus, the interpretation and modalities of how it applies to cyber space should be considered as a priority.

France does not consider the creation of a legally binding instrument to be necessary at this stage. Although there are no international law norms specifically dedicated to cyber space, an evolving interpretation of existing international law, taking into account the effects on States of activities conducted in cyber space, already contributes to enforcing international law.

France continues to promote transparency on doctrines and welcomes the fact that the pre-draft encourages continued exchanges in this area. Each State should be transparent as to its interpretation of the applicability of international law in cyber space in peacetime or more specifically in the context of armed conflict, including as regards the enforcement of international humanitarian law. Affirming the applicability of international humanitarian
law and interpreting its provisions in the light of the technical developments that affect the resources implemented in the context of armed conflict does not mean authorizing or legitimizing the use of force, insofar as this law aims to provide protections to civilians from the effects of hostilities and guarantees to combatants. Transparency does however help increase the predictability of behaviour in cyber space.

However, France considers that principles stemming from international law are not sufficiently mentioned in this section of the document, despite being a constant theme in the discussions. It would be a good idea to reaffirm them. Developments could also be included, especially on the principle of due diligence. France believes it is essential to reach a shared understanding at international level of the obligations on States of which the infrastructure is believed to be being used for malicious purposes against the interests of another State.

In accordance with the principle of due diligence, States have the obligation to not knowingly allow their territory to be used to commit acts prohibited by international law against third States through the use of cyber means. This obligation also applies to activities conducted in cyber space by non-state actors situated in the territory or under the jurisdiction of the State in question. It should be recalled that States must not commit acts prohibited by international law against third States through the use of proxies. A better understanding of how to apply these principles to cyber issues would help bolstering cooperation between States with a view to avoiding conflicts, protecting certain critical infrastructure, and putting a stop to potential major cyberattacks perpetrated via third States. Lastly, international human rights law is only considered through a simple mention of its applicability, whereas the issues of protection of personal data and the use of cyber space as a place to exercise fundamental freedom are today essential.

The issue of the creation of a politically binding framework, as envisaged in paragraph 29, could be accompanied by points to set out what form such an initiative could take, such as whether a plan of action (PoA) is considered.

In paragraph 32, the points on possible technical cooperation on attribution of cyberattacks do not appear relevant at this stage. France considers that attribution is a national and sovereign competence and prerogative. It is up to States to cooperate between one another on these issues if they wish, on an ad hoc basis.

IV. Rules, Norms and Principles for Responsible State Behaviour

In the introductory paragraph of the “Rules, Norms and Principles” section, the notion of “additional specific guidance” used to describe norms seems to be inferior to the level of commitment expected of States. It should at least be underlined that norms enable a clear distinction between acceptable and unacceptable behaviour. As indicated in the general comments, the way the value of norms is expressed should be harmonized throughout the document.

The pre-draft refers to several texts with different statuses in paragraph 36 in order to evoke the genesis of norms. Agreed and universalized elements should not be presented
alongside elements that have been presented to the international community but have not been the subject of agreement.

Several norms proposed in the non-paper attached to the pre-draft report drew our attention. France notes the reluctance of certain States to adopt new norms when elements already agreed are not fully implemented by all. **In the spirit of consensus, the proposals ultimately selected could be those that clarify the norms already agreed in the form of principles or recommendations.** Moreover, France notes an increase of proposals whose scope, status and linkage are sometimes difficult to understand. If the group wishes to include those elements, it will have to work on drafting proposals that are realistic in terms of content and scope.

Paragraph 40 notes that various stakeholders have responsibility for security in the cyberspace. **States should be called on to take the necessary outreach, cooperation and, where necessary, regulatory steps so that the various stakeholders should take their responsibilities, including the public and private sectors and civil societies.**

France reaffirms its commitment to the proposal formulated jointly with Croatia, Finland and Slovenia. States should be encouraged to 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. This aim could be achieved by working with the private sector to define permissible actions using a risk-based approach and to develop concrete tools such as certification processes, best-practice guides, incident response mechanisms and, as appropriate, national regulations.

**France also supports the proposals made by the Netherlands, which are in line with the principles set down in the Paris Call for Trust and Security in Cyberspace.**

**V. Confidence-building measures**

Considerable work on confidence-building measures has been done within the OEWG this year. These discussions appear to be reflected in the current proposals, particularly when it comes to the importance of regional organizations. Within the OSCE, States participate on a voluntary basis in the implementation of confidence-building measures. Engaging in this work and cooperating is also a confidence-building measure in itself. **The drafting of confidence-building measures is essential to create the conditions for serene dialogue between States, to prevent conflicts and to avoid escalation in the event of crises.**

Rather than producing a repository of existing confidence-building measures implemented at regional level, the OEWG would undoubtedly benefit from working with regional bodies in order to draw up guidelines to ensure the effectiveness of such arrangements. For example, it could highlight the relevance of organizing operational exercises, as mentioned in the pre-draft, as well as strategic-level exercises, in order to enable optimal information-sharing and ensure linkage with the political level.

**VI. Capacity-building**
As the report highlights, capacity-building should be a major aspect of international reflection on security and stability in cyber space. Through capacity-building programmes, we can hope to improve global resilience.

We need to foster programmes which, beyond awareness-raising, offer long-term approaches and help support the development of resilient national systems and human resources associated. Effective capacity-building has to be based on programmes created jointly with beneficiaries. Capacity-building programmes also need to be developed for the private sector, which operates a large number of our critical infrastructures. Work on national governance bodies could also help produce more effective and efficient national models. These points should appear in the report.

There is a real lack of resources and there are difficulties matching needs and provisions. Good cooperation and optimal use of resources are one of the major difficulties of capacity-building. It would be useful for the report to more explicitly refer to the institutions outside the UN that could play this role internationally.

VII. Regular Institutional Dialogue

The possibility of “dedicated mechanisms” or the creation of different formats, including an inter-governmental agency, is mentioned in the Regular Institutional Dialogue section. Many States expressed the view that the form should be guided by the content if a specific format were to be created, a point which has yet to be proven. France would like the report to better reflect this concern.

The nature of multi-stakeholder consultations reflects the discussions conducted during the first two sessions. Although the decisions within a working group attached to the United Nations First Committee should be inter-governmental, consultation with the various stakeholders remains essential. Throughout the process, the group would likely have benefited from more discussions in various formats, including with stakeholders which have not traditionally had the opportunity to express themselves within the UN. France supports the inclusion of these points in the final report.

VIII. Conclusions and Recommendations

France would like to thank the Chair and teams for the recommendations which seek a compromise between the positions and proposals of the participating States.

However, France notes that the recommendations contain numerous studies and repositories. The cost, benefits and long-term relevance of such work should be considered. Furthermore, some of the proposed work is already carried out by other institutions, sometimes at regional level, or has already been proposed by the UN, including via UNIDIR. It would undoubtedly be useful to set out a few priorities, and to recommend work on them. That would enable the creation of a document or of a database, instead of a mapping study, that could then be kept up to date. Among the proposals that appear in the report, and as it mentioned during the first two OEWG sessions, France considers that the priority should be to engage the international community in a work on how norms are implemented, in order to refine the
collective understanding of the norms already agreed and enable the drafting of guidelines and
the exchange of best practices. This point has moreover been the subject of a specific proposal
by Australia, Mexico, France, Canada, Chile, Indonesia, South Africa, Pacific Islands Forum
member States, and New-Zealand.

Finally, the proposed mechanism for coordination of capacity-building reflects a real need.
However, it is worth discussing in greater details, particularly to consider the role of the UN
in this area and how it could work with other bodies which are traditionally specialized in the
subject.