Microsoft’s contribution to draft Open Ended Working Group report on cybersecurity

Microsoft commends the United Nations (UN), and in particular the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), for the transparency of their work over the past few months. We especially welcome the publication of the Group’s draft report and the invitation for interested stakeholders to contribute to the work of the Group. The inherently shared nature of cyberspace requires collaboration between and across stakeholder groups to protect the safety and integrity of the online world, and we hope that our contribution provides a useful private sector perspective. We hope that multistakeholder consultations become a key characteristic of all the UN work on cybersecurity.

In our response below, we highlight several cybersecurity challenges that should be addressed by the OEWG as a matter of priority. In particular we underline the importance of cybersecurity capacity building and highlight a set of proposed principles to guide those efforts, welcome the work on confidence building measures in regional organizations, as well as express hope that the conversations on these critical topics in the United Nations will continue in the future. We also strongly endorse proposals for repositories that help clarify how international norms and law apply in cyberspace, and finally highlight a set of proposed norms that we believe would support global stability, in particular in light of the current pandemic.

We also endorse a limited set of new norms proposed by different OEWG stakeholders which we believe are particularly critical. In addition, Microsoft has published a detailed position on the issues under discussion by the OEWG in December and it is available here: https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf.

International law

Microsoft has in the past advocated for member states to issue their own statements on how they interpret and comply with international law, as well as norms in cyberspace. We see examples set by Australia and Canada on their implementation of cybersecurity norms agreed upon in the 2015 UNGGE as a best practice to be emulated by others. Similarly, we welcome statements on interpretation of international law, such as those published, for example, by the Netherlands, France and Australia.

We therefore fully support the recommendation for a repository bringing these statements and positions together, as it would significantly contribute to the collective understanding of how governments interpret their obligations. It would in our opinion encourage member states to proactively issue interpretative statements, as well as provide a useful tool that allows all stakeholders to find and research specific country positions. In addition, references to international norms in international agreements or individual country statements could also be collected. This work could be done under the auspices of the United Nations, or could rely on civil society organizations, such as for example the CyberPeace Institute.

Confidence building measures (CBMs)

Microsoft believes that regional organizations are best placed to share information related to CBMs, as in many cases they are the ones driving work in this space. We are encouraged to see the growing focus of member states on this area and we believe that the priority should continue to be placed on regional and subregional levels rather than at the UN. With that in mind, rather than establishing a repository of such efforts, we would recommend the Secretary General inviting regional organizations to report on their efforts at the next OEWG meeting, and commit to an annual overview of their work in this space.
Similarly, Microsoft believes that Points of Contact represent a helpful tool for increasing resilience and security of cyberspace, as they not only have the potential to improve incident response, but also represent the most fundamental of all confidence building measures – building trust amongst member states. Nevertheless, while in the long-term a global repository should definitely be a desired goal, we recommend first focusing on establishing, maintaining, and utilizing a Points of Contact network at the level of regional organizations. It is clear that the disparate levels of awareness, funding, and resulting capacity, together with cultural differences would make an efficient operation of Points of Contact on a global model difficult. With this in mind, the Organization for Security and Cooperation in Europe (OSCE), or even the European Union, can be utilized as examples of good practice to be emulated in this space. In addition, we recommend ensuring that key industry players are included in these exchanges.

Microsoft has provided an industry perspective to a number of CBMs discussions, including those at the OSCE as well as the European Union (EU), the Organization of American States (OAS), the ASEAN Regional Forum (ARF), and the UN. We encourage the OEWG and GGE to further build on the work in these fora to date to create opportunities for additional confidence building measures and — importantly — focus on implementation of CBMs by providing resources, best practices and (where applicable) funding to less developed states. Moreover, we encourage member states to tap into significant technical and organizational experience in the private sector and civil society to help ensure that CBMs are developed and implemented with multistakeholder input.

Capacity building

No other area under consideration by the OEWG has the potential to make as large an impact on the security and stability of cyberspace as the promotion of cybersecurity capacity building. International law, norms, and confidence building measures can only be implemented and adhered to if member states have the capability and capacity to act on them. However, even with increased attention the supply of such capacity building initiatives continues to fall short of what is needed and efforts are often uncoordinated, both internationally and within countries. Given the limited resources available, as well as the nature of the online environment, well-coordinated international efforts are critical to ensuring at least a common baseline level of resilience and understanding across the globe. That said, and in line with numerous statements made by member states in a variety of international fora, instead of replicating existing efforts, or creating a new global mechanism, Microsoft encourages member states to pool resources to generate greater impact, and participate in fora, such as the Global Forum for Cyber Expertise, which can act as match-making mechanisms between the needs and expertise.

In addition, Microsoft is encouraged to see that the OEWG is looking to develop a set of principles to guide capacity building efforts. Based on our experience in this field, we believe the following framework would substantially help improve capacity building outcomes:

1) **Understand the need.** Capacity building efforts can only succeed if they are responding in a targeted way to a real need. They therefore need to begin with participants’ understanding of what issues matter to them and why, as well as with an understanding of where they have gaps in capacity or capability. Inevitably, these needs will vary depending on regional or local context. Recognition of this dynamic would be welcome guidance to include in any reports developed by the OEWG.

2) **Develop an all of government approach.** All too often, capacity building efforts focus on the technical aspects of cybersecurity at the expense of others – diplomatic, judicial, ... etc. Against the background of the current UN dialogues, Microsoft believes cyber-diplomacy for the foreign service should be prioritized to ensure all member states are equipped to participate in the conversations on a more equal footing.
3) **Be culturally responsive and ensure initiatives locally owned.** While we increasingly all connect to the same public Internet, the ways in which we use modern technology and the way we learn new information is heavily influenced by local customs and cultures. With this in mind, it is critical that capacity building efforts consider the local context and ensure that recipients are bought into the process.

4) **Maintain relevance of capacity building.** Technology is evolving rapidly. And it is important to ensure that capacity building efforts move with the times. Trainings should therefore strive to incorporate understandings of the latest technologies. Even more importantly, capacity building needs to be treated as a continuous process, rather than a one-off engagement.

5) **Be inclusive of all stakeholders.** It is critical that capacity building focuses not just on government stakeholders, but industry and civil society as well. Moreover, effective cybersecurity capacity building programs also rely on the support of government stakeholders as well as industry and civil society organizations with relevant expertise to develop trainings, exercises, and other initiatives. This essential multistakeholder dynamic in capacity building – in both delivering and receiving – should therefore be recognized in any guidance produced on the subject by the OEWG.

**UN Processes**

Microsoft is also encouraged to see the recommendation for the 76th session of the General Assembly to convene a new open-ended working group of the General Assembly and request the Secretary-General to establish a new group of governmental experts. To us it is clear that a continued institutional dialogue on this important topic is pivotal. However, it is also important to note that this process needs to create a consistent, meaningful role for industry, academia, and civil society participation – alongside governments and other institutions. The development of norms and rules will benefit significantly from a multistakeholder approach, as dialogue restricted to government participants does not reflect the input or expertise of communities that directly manage ICTs or that have experience advocating for peace and security across a range of contexts and issues.

The decision to include a multistakeholder community during the December intersessional meeting of the OEWG was a significant step forward in this regard, and we appreciate as well the regional multistakeholder consultations of the GGE. However, multistakeholder inclusion in these dialogues has not been consistent and continues to be ad-hoc, limiting the potential benefits of regularized ongoing collaboration. To this end, establishing a formal consultative process for the GGE, and a formal participation structure for the multistakeholder community in the OEWG, would be to the benefit of both dialogues.

**New norms and principles**

Finally, it is clear that the existing “Framework for Responsible State Behavior in Cyberspace”, comprised of the 2010, 2013 and 2015 GGE consensus reports, has been insufficient thus far to prevent the escalating numbers of sophisticated cyberattacks we see today. New norms and principles should be considered to clarify expectations for responsible state behavior and to keep pace with the evolving nature of cyber threats. We are therefore encouraged to see that a number of countries and other actors have put forward proposals in this space and therefore below highlight those that we hope member states take up as subject of further discussion. At the same time, we believe it is important that the work of the OEWG and the Group of Governmental Experts (GGE) remains complementary, that both groups reinforce each other, and that the existence of two processes should in particular not be used as an excuse to “forum shop”. We therefore encourage the Chairs of OEWG and GGE to agree a uniform approach to these proposals, one that ensures important norms are adopted and then implemented across the world.
Recent events have made one of the norms that has been proposed particularly relevant: The International Committee of the Red Cross put forward the following proposal: “Norm prohibiting states from conducting or knowingly supporting ICT activity that would harm medical services or medical facilities, and would oblige them to take measures to protect medical services from harm.” While these protections exist in times of armed conflict, paradoxically, they do not yet exist in peacetime. That is an unacceptable state, in particular as the world fights a dangerous, yet invisible enemy – Covid-19 – we should ensure that these efforts are not undermined by a second invisible enemy – cyberattacks. The fact that in the month of March alone, hospitals, medical facilities, government health agencies, and testing centers, and even the World Health Organization, have faced targeted cyberattacks perpetrated by malicious actors, clearly signals that this norm is timely and needed. We urge member states to adopt it as part of their OEWG deliberations. In addition, member states and other participants in the OEWG process should act swiftly by issuing statements of support for this norm while also committing to refraining from any such activity.

In addition to the ICRC-proposed norm, Microsoft strongly supports several of the new norms that have been proposed by member states which we believe are critical additions to the existing foundation of cyber norms previously agreed in the GGE context:

- 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.
- State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.
- States should increase exchanges on standards and best practices with regard to critical infrastructure protection and encourage enterprises to embark on such exchanges.
- States should pledge not to use ICTs and ICT networks to carry out activities which run counter to the task of maintaining international peace and security.

In addition to the proposals highlighted by various UN member states, other actors in the multistakeholder community have put forward proposals for new principles and norms. Unfortunately, these have not been reflected in either the draft report or its annex. In particular, we urge governments to consider proposals introduced by the Global Commission for the Stability of Cyberspace and also those put forward in the Paris Call for Trust and Security in Cyberspace. The Paris Call builds on the previous GGE reports, but also includes 3 new principles, some of which are, at least in parts, reflected in government proposals above:

- Prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;
- Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;
- Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.

We hope these responses provide a helpful contribution in advancing a shared objective: achieving a rules-based and rights-respecting online world for all. Accomplishing this requires trust and cooperation across stakeholder groups with responsibilities in this space, underscoring the value of precisely this sort of outreach. We are grateful for the opportunity to contribute to this important process and we look forward to additional opportunities to collaborate in the future.