Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

LIST OF GUIDING QUESTIONS AND NON-EXHAUSTIVE LIST OF INFORMATIVE DOCUMENTS FOR THE FIRST SUBSTANTIVE SESSION, 13-17 DECEMBER 2021

Microsoft's submission

Microsoft would like to commend 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. We hope that the OEWG will recognize the inherently shared nature of cyberspace in its future deliberations and acknowledge the need for collaboration across stakeholder groups to protect the safety and integrity of the online world.

In our submission below, we include a small subsection of what we believe are issues that should be addressed by the OEWG as a matter of priority, as well as single out norms that have been proposed by different stakeholders in recent weeks, and we believe are worth considering. We hope these recommendations provide a helpful contribution to advance a shared objective: achieving a rules-based and rights-respecting online world for all. Please let us know if we can provide any additional input or clarify any of the contributions provided here and we look forward to additional opportunities to collaborate in the future.

General questions that States may wish to address during the general exchange of views

1. Many States have called for an action-oriented approach. How can the OEWG be an action-oriented process and deliver tangible results to States while building on previous outcomes?

Define actionable outcomes, set deadlines and hold each other accountable

Microsoft believes that the easiest way to deliver on an action-oriented approach is to work on implementation of previous agreements – both as it relates to norms and international law. Individual States have already put forward suggestions and positions as to how implementation could be supported as part of the previous OEWG and Group of Governmental Experts (GGE), but we believe that the current OEWG could accelerate those approaches, including e.g. by encouraging more countries to share voluntary national contributions on the subject of how international law applies to the use of ICTs.[1]

Moreover, we believe that clear targets and deadlines foster accountability, which in turn is the best guarantee for delivering tangible results. To foster it, we recommend for the OEWG Chair to add a sub-item to Agenda item 6 ("Other matters"), outlining "Deliverables for the next substantive session". With that in mind, we recommend that throughout the December deliberations, and with the help of the Secretariat, the Chair compiles an overview of action items pertaining to either individual law or norm implementation. These action items could include initiatives within States or look to enhance implementation through capacity building efforts.

In a year's time, States would be expected to provide a brief overview, in writing, of the progress made. These efforts would highlight good practices, drive accountability, but also build momentum. The Chair would also be able to compile interim reports focusing on these clear deliverables on an annual basis, ensuring that the final report is not the only outcome of the OEWG.

[1] A-76-136-EN.pdf (un-arm.org)

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

2. Are there specific issues that require urgent attention and early outcomes, bearing in mind the need to address all issues on the agenda in a balanced and comprehensive manner?

Drive wholistic progress on all priority topics

Microsoft strongly believes that all issues on the table today are equally deserving of both time and attention. Urgent progress is needed across all of the topics identified as priority as part of the OEWG.

With that in mind, Microsoft recommends that the OEWG keeps all the outlined topics on the agenda of each of the upcoming substantive sessions – and that the Chair as well as States commit and push for progress between each of the substantive sessions. That way, progress – as well as lack thereof – can be tracked from session to session and the Chair as well as the States can hold each other accountable.

That said, given global and geopolitical realities, we would be remiss not to stress that, in light of an ongoing global pandemic, particular attention should be paid to the effects of threats emanating from cyberspace on the healthcare sector and to work towards adequately protecting it from cyber harm.

3. Given the unique role that stakeholders play in cyberspace, how can the OEWG engage them meaningfully and substantively in order to support discussions by Member States and deliver tangible results?

Engage with stakeholders in a systematic, sustained and substantive manner

Microsoft agrees wholeheartedly with the Chair that stakeholders play a unique role in cyberspace and that threats in this space cannot be tackled by States on their own. Indeed, States should consult widely with the entities that develop and operate many of the technologies rely on – as individuals, organizations, and countries. In the past, this inclusion has already proven fruitful, not only through the previous OEWG's Intersessional Meeting in 2019, but through the plethora of informal consultations that have built trust amongst and across stakeholders since then.

Against that background, we were pleased to see the efforts of the Chair to schedule informal consultative meetings ahead of each of the substantive sessions of the OEWG. This represents a good start, in particular if accommodations could be made for members of the multistakeholder community that cannot travel to New York – either because of funding or healthcare constraints. However, to meet the Chair's stated commitment for "engaging with stakeholders in a systematic, sustained, and substantive manner", which aligns with views from a number of States, more needs to be done.

While including the multistakeholder community formally in UN processes on cybersecurity might be a relatively new concept, we encourage the Chair to draw on recent successful examples like the Paris Call for Trust and Security in Cyberspace[2] – where governments, industry and civil society worked side by side to endorse a set of principles and elaborate their implementation. In particular, we would like to reference the outcomes of Paris Call working groups #3 (on multistakeholder participation at the UN)[3] and #4 (on advancing international norms)[4], respectively. We hope that the Chair is open to replicating that model and that multistakeholder inclusion will be expanded so as to ensure meaningful participation of all interested parties throughout the OEWG process. With that in mind, we propose the following options for consideration:

- Consulting on actionable proposals with the multistakeholder community;

[2] https://pariscall.international/en/

[3] https://pariscall.international/assets/files/10-11-WG3-Multistakeholder-participation-at-the-UN-The-need-for-greater-inclusivity-in-the-UN-dialogues-on-cybersecurity.pdf

[4] https://pariscall.international/assets/files/WG4-Final-Report-101121.pdf

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- Organizing side events and round tables, in cooperation with States and the Secretariat;
- Exploring opportunities for an ongoing exchange of information to address pressing challenges;
- Ensuring that the multistakeholder community is able to – if not participate in – at least follow State deliberations.

Unfortunately, when it comes to the current arrangement we are concerned that the restrictive accreditation processes for multistakeholder participation runs the risk of excluding organizations with valuable perspectives that may not be traditional participants in UN forums. Therefore, it is critical that any accreditation for the OEWG goes beyond the strict inclusion of groups that are already accredited at the Economic and Social Council (ECOSOC), or those that have a standing invitation to participate as observers at the General Assembly.

One way to achieve this could be for the OEWG to mirror the approach adopted recently by the Cybercrime Ad Hoc Committee. The Chair of the Ad Hoc Committee has recently invited any organization with an interest in the subject to submit a request to participate. The applicants will be of course vetted, but any objection to an organisation's participation would require a public elaboration of the rationale behind that decision.

We also encourage the Chair to leverage technology as much as possible to encourage remote participation in debates. As mentioned above, technology allows for a wider participation, both when it comes to questions of healthcare and funding. While we recognise that in-person meetings can be fruitful when it comes to building consensus and negotiating details, virtual meetings much more inclusive. We therefore recommend that all formal meetings be live streamed, recorded, and published on the relevant UN websites.

Another important element is transparency in information sharing. Microsoft believes that transparency and openness need to be at the centre of all UN discussions on cybersecurity. Timely sharing of documents, agendas, and information in general is the baseline on which effective multistakeholder cooperation can be built. Without it, potential participants in the dialogue, including governments, simply cannot participate in an informed and meaningful manner.

Fortunately, technology has simplified information sharing, a fact that the United Nations Office for Disarmament Affairs (UNODA) has made full use of as part of the previous OEWG. We hope that UNODA builds on those efforts, enhances its existing platform, and continues to publish information around the ongoing process, as soon as possible. The types of information that can be made public could include:

- Meeting agendas;
- Official documents produced by the Secretariat;
- Official communication to States;
- Individual submissions by States or non-governmental actors to the ongoing dialogue;
- Contact details of the Secretariat;
- Contact details of the participating State representatives.

We would like to strongly advocate for the opportunity to provide direct input into the deliberations. With that in mind, a mechanism needs to be set up that will allow representatives of non-governmental organizations to provide input – orally and in writing.

The previous OEWG on cybersecurity went some way towards making that happen. The Secretariat ensured that the submissions of the multistakeholder community that were shared with them were published on the appropriate website and ensured that state representatives were aware of them. However, it was somewhat difficult to understand what documents were open for consultation and what

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

the deadlines were. We encourage this current OEWG to build on these efforts, retains the positives aspects of the previous process and works to improve the written consultation procedure.

Lastly, while it is critical to focus on multistakeholder participation during UN negotiations on what the rules of behaviour for States should be, transparency and inclusion of different perspectives are equally important in the discussions about their implementation. We hope that the Chair takes the opportunity to encourage States to consult widely as part of their domestic implementation processes.

Continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats

1. **Noting the extensive discussions on existing and potential threats, what are some examples of urgent and challenging existing and potential threats that States are facing**?

Focus on State-level threats

This past year has brought powerful reminders that to protect the future one must understand the threats of the present. This requires the continuous sharing of data and insights. Certain types of attacks have escalated as cybercriminals and other sophisticated actors change tactics, leveraging current events to take advantage of vulnerable targets and advance their activity through new channels.

Looking at the threat landscape, along with data and signals from across its company teams, Microsoft has identified five top-level areas which have emerged as most critical today: cybercrime (ransomware in particular); State based threats; supplier ecosystems, Internet of Things (IoT), and operational technology (OT) security; the hybrid workforce; and disinformation.[5] Juxtaposing the above against the mandate of the OEWG, we recommend a strong focus on State threats.

2. **What capacities and structures are needed at the national level to prevent, detect, and respond to existing and potential threats? What can the OEWG do concretely to facilitate the building up of such capacities at the national level?**

Avoid duplication of efforts and foster complementarity by building on existing initiatives

Microsoft encourages the OEWG to appropriately recognize existing capacity building initiatives that operate outside the UN system, such as the Global Forum on Cyber Expertise (GFCE)[6], so as to foster complementarity and avoid duplication of efforts. Moreover, any serious effort to improve capacities and uphold a rules-based order in cyberspace will require meaningful involvement of and cooperation with all relevant stakeholder groups.

3. **How can we apply the existing framework of agreed measures from previous OEWG and GGE reports, including norms, to deal with existing and potential threats? How can we enhance the application of the framework of agreed measures?**

Identify and understand the threat landscape, implement agreed measures and hold each other accountable

[5] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

[6] https://thegfce.org/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

To effectively deal with existing and potential threats, it is necessary to first identify and understand these threats. Here, too, the involvement of all relevant stakeholders is essential – including civil society, academia, technology researchers and industry. For example, Microsoft's threat assessment is based on more than over 24 trillion daily security signals and it leverages both AI powered predictions as well as the expertise and insight of human analysts. As such, any sincere discussion of existing and potential threats must, as a prerequisite, include meaningful participation from all relevant stakeholders.

Moreover, to enhance the application of the framework of agreed measures, we recommend that the OEWG places particular emphasis on implementation. As previously mentioned, this could include an exchange of views and good practices and identify models that would support the incorporation of existing agreements in national contexts. That said, we reiterate that a critical component of those conversations needs to be focused on the sharing of good practices regarding effective multistakeholder participation, both domestically and internationally.

Looking ahead, the successful application of any framework requires a viable mechanism tasked with overseeing its implementation. Looking at both the status quo and the trends related to threats emanating from cyberspace, it is unlikely that these threats will diminish, let alone disappear. As such, the OEWG, with its time-bound mandate, can be a much-needed catalyst and the next step in the right direction. That said, to make meaningful progress over time, the OEWG should, from the outset, consider how its provisions could feed into a permanent, regular institutional dialogue with the broad participation of States – and to also consider how such a dialogue could be set up so as to allow for meaningful multistakeholder inclusion.

4. How are existing and potential threats experienced differently by countries and different segments of society? How can the OEWG address the differentiated impact?

Drive deeper understanding of the differentiated impact online threats have

Microsoft respectfully defers to countries themselves to outline how they are experiencing existing and potential threats emanating from cyberspace. However, any sincere effort to learn about how different segments of society are experiencing these threats, must, as a prerequisite, provide the segments in question – along with all relevant stakeholders that make up these segments – an opportunity to showcase their experiences. One example of the work being done in this space is the research into the implications on the healthcare sector that the CyberPeace Institute[7] is driving, highlighting the long-term consequences of cyberattacks on the provision of medical care.

To this end, we encourage the Chair to consider venues for sharing these experiences, in addition to the informal consultative meetings that have already been proposed. For example, stakeholders could be invited to share their experiences in writing, and have these submissions included on the OEWG website, for transparency and have this feed into the deliberations during the substantive sessions of the OEWG. The Chair could also consider hosting additional – and for the sake of inclusion likely virtual – sessions that focus on the various segments in questions.

For example, and as mentioned above, the most recent Microsoft Digital Defense Report identified five top-level areas which have emerged as most critical today: cybercrime (ransomware in particular); State based threats; supplier ecosystems, Internet of Things (IoT), and operational technology (OT) security; the hybrid workforce; and disinformation.[8] Clearly, these threats are impacting countries across the globe differently and to varying degrees. That said, a concrete way in which the OEWG could address these differentiated impacts would be to provide Member States with opportunities to share their

[7] https://cyberpeaceinstitute.org/healthcare/

[8] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

experiences and the steps they have taken to mitigate the various threats. This would empower the OEWG to better discuss possible countermeasures, especially if views from other stakeholders were also allowed to contribute in a meaningful manner.

5. What are other aspects the OEWG should consider with regard to this topic?

Work with all relevant stakeholders to tackle threats emanating from cyberspace

Microsoft believes that, in light of this growing trend and the threat it poses, the OEWG should consult on and identify potential avenues to limit the use of private sector offensive actors (cyber mercenaries) in cyber conflict to mitigate risk. This work could start addressing current ambiguity around not just what tools and techniques should be banned, but also setting clear boundaries around intent, authority and intrusiveness.

Further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour

1. How can States better survey their national efforts to implement norms and assist each other in this endeavour? What can the OEWG do to facilitate the conduct of national surveys on norm implementation?

Incentivize States to survey national efforts, set deadlines and encourage transparency

Implementation of norms by States requires two key prerequisites – namely (a) the political will and (b) the capacities to do so in a meaningful manner. Microsoft believes that the OEWG can play a critical role related to both prerequisites.

First, it can incentivize States to survey their national efforts by setting a deadline by which they should have completed an initial survey of their national efforts to implement norms and invite States to publish these findings on the OEWG website or through the UNIDIR Cyber Stability Portal. This should build on the survey initiative previously proposed by Australia and Mexico. A reasonable deadline for such a first assessment could be the 4th substantive session of the OEWG, scheduled for March 2023.

Second, we encourage the OEWG to invite stakeholders to regularly measure progress made on norm implementation. Technology will evolve as will the understanding on how to foster stability and security of cyberspace. With that in mind, we urge the OEWG to work towards ensuring that implementation of cybersecurity norms is not a one-off investment, but a continuous process. In concrete terms, the OEWG could invite Member States to measure whether they are making progress in implementation of norms and share their progress with the group, in a transparent manner.

Third, the OEWG should facilitate the provision of assistance to States who currently lack the capacity to meaningfully pursue the above points. Such assistance could come in the form of multilateral support but could also leverage the experience, expertise and resources from other stakeholders. Concretely, the Chair could convene, in addition to the already foreseen informal consultative meetings with stakeholders, a set of meetings – open to all relevant stakeholders – that focuses on building the necessary capacities of States. Forums such as the abovementioned GFCE could also play a critical role in this endeavour.

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

2. How can the OEWG facilitate the sharing of experience and good practice on norms implementation at the national and regional/sub-regional levels?

Build on existing efforts, avoid duplication and foster complementarity

We believe that it is important that whatever the OEWG does in this space adds to the ongoing efforts and does not seek to replicate them. As such, the Chair could leverage the convening power of the OEWG to invite States as well as regional-, and sub-regional organisations to share their good practices and lessons learned on a regular basis. With this in mind, these updates could be collected on an annual basis, so that the OEWG could take stock of and be informed by these endeavours, as well as benefit from the lessons learned.

3. What concrete actions have States undertaken to strengthen measures to protect critical infrastructure from ICT threats? How can the OEWG facilitate the exchange of good practices with regard to critical infrastructure protection?

Incentivize States to share information and learn from each other

Microsoft respectfully defers to States to report on the actions they have taken to strengthen measures to protect critical infrastructure from ICT threats. That said, to enable States to learn from each other, the OEWG Chair could invite States to compile their actions – at a high-level and obviously including non-classified information only – and post them on the OEWG website. A reasonable deadline for these submissions could be the second 3rd substantive OEWG meeting, currently scheduled for July 2022.

Moreover, with the help of the OEWG Secretariat – and, potentially with the support from other interested stakeholders – a Compendium of these actions and good practices could be compiled and widely disseminated, so as to further raise awareness and build the necessary capacities.

That said, we respectfully remind the OEWG that protection of critical infrastructures in only one of the eleven norms previously agreed by States. We therefore encourage the OEWG to place appropriate attention to the remaining norms as well.

4. Based on States' experience in implementing the norms and taking into account previous OEWG and GGE reports, is there a need to further elaborate the existing norms or to consider the development of additional norms over time? If yes, what are the key issues that the OEWG should address?

Implement existing norms and work to identify potential gaps and explore the need for new norms

While the existing normative framework represents an important contribution to the stability of the online environment, it is Microsoft's view that there remain several gaps in the international cybersecurity framework that attackers continue to exploit. It is likely that as technology evolves, even more of these will become apparent. Looking at the current threat environment, we urge States to consider the development of additional norms on (a) protecting the healthcare sector from cyber harm and (b) protecting the supply-chain, especially with regard to software update mechanisms.

Increasing cyberattacks on the healthcare sector, including on vaccine research entities, during a global pandemic, have illustrated that this sector is both valuable and vulnerable enough to warrant specific, dedicated provisions that go beyond what is currently specified in the acquis. Similarly, sophisticated government actors have repeatedly targeted the technology supply chain to carry out attacks, including through the exploitation of routine software update processes. These update exploits are a particular threat to public trust and confidence in technology as update mechanisms underpin the security and maintenance of many digital products and services. We believe that supply chain attacks that target

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

software updates are distinct enough to require further elaboration and specific recognition in norms discussions.

Importantly, further clarification of existing norms or the potential elaboration of new ones over time in this space should benefit from the input of all relevant stakeholders, including the private sector, civil society and academia.

5. What role might other stakeholders such as the private sector and the technical community play in the implementation of norms?

Provision of insights into threats and possible technical solutions

Threats emanating from cyberspace cannot be tackled by States alone. It is Microsoft's view that as one of the vehicles aiming to increase the stability of cyberspace, international cybersecurity norms also cannot be elaborated and implemented by States alone. This view is reflected in a number of initiatives in this space that have been developed over the past decade, for example the Paris Call for Trust and Security in Cyberspace, which is now endorsed by more than 80 States and more than 1200 stakeholders across governments, industry and civil society in total. The initiative has already resulted in work on a compendium on advancing international norms[9], a compendium on countering election interference[10], a compendium on cyber hygiene[11], and a policy guide on no hacking back[12].

The technical community and the private sector are particularly well placed to provide information around the threats emerging from cyberspace, help with understanding of the technical solutions (existing and possible), as well as elaborating on the impact certain policy decision make have on the end user. As the private sector operates the majority of the technical infrastructure globally, those discussions will be particularly important both on elaboration and implementation of norms. We encourage the OEWG to leverage this knowledge, by providing the multistakeholder community an opportunity to meaningfully contribute to OEWG deliberations.

6. What are other aspects the OEWG should consider with regard to this topic?

Leverage and build on work done by the multistakeholder community and regularly measure progress

Throughout its efforts, the OEWG could more systematically try to reflect the work that is already under way but has been developed or implemented in multistakeholder fora. For example, it could build on initiatives, such as the Paris Call for Trust and Security in Cyberspace[13], in particular its Working Group 4 on Advancing International Norms[14]. Efforts such as these have put forward potential models for multistakeholder cooperation for identification of good practices, as well as highlighted good practices to drive implementation.

Similarly, we would suggest that the OEWG encourages States to regularly measure progress made on norm implementation. Technology will evolve as will our understanding on how to ensure stability and security of cyberspace. With that in mind we should ensure that implementation of cybersecurity norms

[9] https://pariscall.international/assets/files/WG4-Final-Report-101121.pdf

[10] https://www.canada.ca/content/dam/di-id/documents/compendium-eng.pdf

[11] https://cybertechaccord.org/uploads/prod/2020/11/Cyber-Hygiene-Appendium-update-191120-pages.pdf

[12] https://cybertechaccord.org/uploads/prod/2020/11/hack-back-update-131120-pages.pdf

[13] https://pariscall.international/en/

[14] https://pariscall.international/assets/files/WG4-Final-Report-101121.pdf

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

is not a one-off investment, but a continuous process. The OEWG could build on the implementation survey highlighted above to create a mechanism that would allow States to measure whether they are making progress in the implementation of norms, but more importantly in improving their security posture. Such a mechanism should be tailored to local contexts.

How international law applies to the use of information and communications technologies by States

1. **States are encouraged to inform the Secretary-General of their national views on assessments on how international law applies to their use of ICTs in the context of international security. How can the OEWG facilitate the sharing of such national views and practices, including through existing tools such as the UNIDIR Cyber Policy Portal?**

Leverage the OEWG's "forcing function" and drive greater transparency and understanding

The OEWG can act as a "forcing function" by creating mechanisms that would hold States accountable for producing their national positions, albeit on an informal basis. For example, the Chair could encourage States to publish their national assessments on how international law applies to their use of ICTs in the context of international security. This could be done in line with a clearly defined deadline, for example the start of either the second or third substantive session of the OEWG, and at that point the positions would be shared broadly and uploaded on UNIDIR's Cyber Policy Portal. Moreover, the Secretariat could informally encourage States to respond, by engaging with them on the topic regularly, producing templates, reminding them of relevant deadlines, etc.

More broadly, we encourage the OEWG to drive greater understanding of how international law applies to cyberspace. We would like to reiterate our position that norms are only one part – albeit a crucial one – of the international cybersecurity framework that states need to abide by. International law, including international human rights law, and international humanitarian law complete the puzzle.

With that in mind, the OEWG should not only encourage States to articulate their positions, but seek to promote initiatives that look to clarify the status quo, and drive capacity building at the same time. Multistakeholder work in this space, in academia and beyond, could be particularly helpful in this regard. For example, the Oxford Process on International Law Protections in Cyberspace[15] has held numerous convenings to discuss the practical application of legal concepts and produced statements that reflect consensus in this space.

2. **How can the OEWG facilitate the further study of and discussions on how to deepen common understanding on how international law applies to State use of ICTs? Which specific rules and principles of international law applicable to State ICT use merit further study?**

Leverage multistakeholder insights related to international law and build on their outcomes

In paragraph 37 of the Final Substantive Report[16] of the previous OEWG, States concluded that "there was a need for additional neutral and objective efforts to build capacity in the areas of international law, national legislation and policy".

One such effort, is the Oxford Process on International Law Protections in Cyberspace[17], mentioned above. At the core of this initiative lies a collaborative effort between international legal experts from

[15] https://www.elac.ox.ac.uk/the-oxford-process#/

[16] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[17] https://www.elac.ox.ac.uk/the-oxford-process#/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

Microsoft

across the globe aimed at the identification and clarification of rules of international law applicable to cyber operations across a variety of contexts.

The rationale behind the Oxford Process is to not discuss the theoretical frameworks of international law, but to discuss and demonstrate how the latter can be applied to and used in real world situations today. Discussions focus on a particular topic – for example vaccine research – and elaborate on the obligations and prohibitions that can be leveraged to protect a particular sector. The Oxford Process has thus far produced five so-called "Oxford Statements" – each signed by more than 100 legal experts – on International Law Protections against Cyber Operations targeting the Health Care Sector[18], Safeguarding Vaccine Research[19], International Law Protections against Foreign Electoral Interference through Digital Means[20], the Regulation of Information Operations and Activities[21], and the Regulation of Ransomware Operations[22].

We recommend the OEWG invite representatives from the Oxford Process, as well as other similar initiatives that deal with issues related to in international law, to brief States during an upcoming substantive session. Moreover, we recommend States to consider funding, putting forward specific and pertinent topics that would be worthwhile examining by international legal experts, and engaging in such discussions.

3. What additional capacity is needed e.g., in the areas of international law, national legislation and policy, to enable all States to further contribute to building the common understanding of how international law applies to the use of ICTs by States?

Build capacity through focused trainings and deep dives into different subject matters

International law is an important tool to ensure perpetrators are held accountable for their malicious actions in cyberspace, and it is particularly pertinent when it comes to cyberattacks associated with State actors. As mentioned elsewhere, Microsoft believes that it would be important to leverage it more often than is common today, but we also understand that not all States have the necessary capacity to do so. As such, we encourage more States to fund training courses on the applicability of international law in cyberspace, e.g., akin to what is currently being developed by Canada. The OEWG could help promote and coordinate these types of trainings.

Other efforts that could be pursued include initiatives such as the aforementioned Oxford Process, or other trainings for government legal experts that go deeper into a particular subject and help them think through how international law applies to a particular situation. It is pivotal that these include industry, academic and civil society perspectives, ensuring the approaches are truly multidisciplinary and reflective of real life. These could then feed into national statements, policy and positions on this topic, ultimately building a common understanding of how international law applies in cyberspace.

4. What are other aspects the OEWG should consider with regard to this topic?

---

[18] https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea

[19] https://www.elac.ox.ac.uk/article/the-second-oxford-statement

[20] https://www.elac.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through

[21] https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities

[22] https://www.elac.ox.ac.uk/the-oxford-statement-on-ransomware-operations

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

Clearly state what aspect(s) of international law and norms were breached when attributing cyberattacks

As mentioned earlier, Microsoft believes that it is important to not only discuss how international law applies to this space, but to ensure that it is leveraged appropriately. We therefore urge States to not only call out malicious actors, but to also explain in their attribution statements what aspect(s) of international law and norms has been breached. With that in mind, we encourage the OEWG to discuss specific situations and cases, as well as hypothetical ones, to ensure that States are better prepared to incorporate such considerations in future attribution statements.

Confidence-building measures

1. **What confidence-building measures have been identified and which have been practically implemented by States at the bilateral, regional, or multilateral level? How can the OEWG further facilitate the exchange of lessons and good practices on confidence-building measures?**

Build on existing CBMs, but also include other stakeholders in their implementation

Microsoft recognizes the importance of Confidence-Building Measures (CBMs) as tools to reduce tension, minimize the risk of misperception, and to build trust. CBMs can act as a pressure valve and can therefore help deescalate critical situations. Notable agreements in this realm include the various sets of cybersecurity CBMs agreed to by participating States of the Organization for Security and Co-operation in Europe (OSCE)[23]. It is worth noting that, to a certain extent, a mechanism such as the OEWG can, arguably, be considered as a CBM in and of itself.

That said, rather than call out any specific measure, we would like to make an overarching comments, applicable to CBMs as a whole. In the 21st century, both the implementation of existing CBMs as well as the elaboration of potential new ones, would benefit from a meaningful inclusion of all relevant stakeholders. As such, we reiterate our call for the OEWG to broaden the information exchange and communication to all relevant stakeholders (see also bullet point #5 of this section).

2. **How can the OEWG facilitate support for States to engage in transparency measures, such as by sharing relevant information and lessons learned including through the UNIDIR Cyber Policy Portal?**

Incentivise regular updates, leverage UNIDIR tools and hold each other accountable

Microsoft believes that the OEWG can provide a "forcing function" for States to act, implement and publicly report on their transparency measures and lessons learnt. As proposed earlier in the document, the Chair could encourage States to report on their deliverables on an annual basis, which would both create a deadline for them to meet, and thereby hold States accountable.

Moreover, we would encourage States to fund the UNIDIR Cyber Policy Portal further to ensure that they can provide an effective Secretariat for the implementation of the commitments. It is our experience that having a Secretariat to engage with individual States, remind them of the deadlines, and help answer any questions is the most effective way to ensure regular reporting and updates are provided.

[23] https://www.osce.org/secretariat/cyber-ict-security

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

3. How can the OEWG facilitate support for States in nominating a Point of Contact, inter alia, at the technical, policy and diplomatic levels? How can the OEWG facilitate the coordination and information sharing among designated Points of Contacts?

Establish meaningful Points of Contact and empower them so they can fulfil their responsibilities

As highlighted throughout this section, Microsoft believes an up-to-date, global list of Points of Contact would be a worthwhile endeavour. As mentioned elsewhere, we do not necessarily believe that the UN needs to reinvent the wheel and create its own list from scratch, but build on successful efforts in regional fora, such as the EU or OSCE in particular (see next question).

For simplicity's sake we would suggest that governments each nominate a Point of Contact and an alternate and do not necessarily nominate individuals across the technical, policy, and diplomatic levels. Nevertheless, we would support the OEWG encouraging States to nominate leads across those areas domestically and ensure that their international Point of Contact can refer to them should the need arise. This database could be used to facilitate general information sharing and in crisis response.

Importantly, given its convening power, we encourage the OEWG to not only focus on the nomination process, but to also to facilitate regular exchanges between these Points of Contact through virtual trainings or exercises. These could be organised annually, so that contacts have a chance to meet and get to know each other before a crisis erupts. This approach fosters the necessary trust-building that is vital for effective and efficient communication during a potential crisis.

4. Are there successful examples of a network or directory of Points of Contact? How can the OEWG facilitate the sharing of best practices and experience, and the application of a network and directory at the global level?

Learn from and build on existing examples

As previously indicated, various examples of Points of Contact in this space exist. Of course, some are more effective than others, but that largely depends on how diligent the organizations that maintain the lists have been in ensuring that these are kept up to date, that exercises take place to demonstrate their utility, as well as that these are leveraged when necessary.

Rather than reinvent the wheel and create a new list at the global level, we encourage the OEWG to learn from and build on the regional experiences. To that end, we would recommend the Chair works with the regional organizations in question to identify good practices, gaps that exists, as well as models that could ensure that current frameworks could be leveraged to build a global directory. Relatedly, the OEWG should consider establishing regional liaisons through cooperation with regional organization to drive international collaboration in prevention, response and recovery efforts. This could facilitate coordinated initiatives down the line and offer tailored regional support for States.

Moreover, we believe a consultation process with States that have contributed to and, ideally, actively participated in these various other Points of Contact initiatives would be beneficial. Similarly, it would be worthwhile elaborating how the different States coordinate these types of efforts at national level.

5. What are other aspects the OEWG should consider with regard to this topic?

Learn from regional efforts and take them to the global level

Over the past few years, Microsoft has provided an industry perspective to a number of CBMs efforts, including those held at the OSCE, as well as the European Union (EU), the Organization of American States (OAS), the ASEAN Regional Forum (ARF), and at the UN. We have done that with the objective of

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

identifying new measures, in particular those that bring in industry perspectives, as well as to help ensure effective implementation of existing measures.

Against that background, we encourage the OEWG to learn from these regional efforts, identify good practices, and encourage their adoption across the globe. Moreover, Microsoft encourages States to broaden their view of cybersecurity CBMs and move beyond conversations that are limited to States only. Effective future CBMs in this space need to be informed by the experience and expertise of all relevant stakeholders, which of course requires their meaningful inclusion in the relevant discussions.

Capacity-building

Which areas of capacity-building support should be prioritized for early action or urgent implementation? For example, in the following areas: Developing and implementing national ICT policies, strategies, and programmes; Creating and enhancing capacity of CERTs and arrangements for cooperation; Improving security, resilience, and protection of civilian infrastructure; Building technical, legal and policy capacities of States to detect, investigate and resolve ICT incidents; Deepening common understandings of how international law applies to the use of ICTs by States; Enhancing technical and legal capacities to investigate ICT incidents; Implementation of voluntary norms.

Commit to a sustained capacity building effort over time

Cybersecurity capacity building cannot be seen as a one-off initiative, rather it must be seen as a sustained commitment over time by all the entities and individuals participating. Technology develops with some speed and therefore any implementation effort needs to be refreshed and updated regularly. This is true for national priorities and frameworks, as well as CERTs, incident response, or any of the other areas that were highlighted in the consultation. We therefore do not recommend the OEWG prioritizes one area over another as part of its work program.

Instead, we recommend the OEWG to map existing capacity building initiatives and resources under each of the topics identified and work with their "creators" to make them available to the international community. Moreover, we hope that the OEWG goes further and works on identifying any gaps in cybersecurity capacity building efforts, working with the recipients of these efforts to understand what they would find as particularly helpful. These newly identified areas could then serve as potential areas for collaboration with the multistakeholder community, as they could offer potential solutions to address those gaps.

Importantly, we encourage States to be mindful of existing capacity building initiatives and to promote coordination and resourcing of such efforts. We further encourage States, in line with previous OEWG recommendations, to continue informing the Secretary General of their views and assessments related to capacity building in this space, including on relevant lessons learned and good practices.

1. **What are some of the capacity-building initiatives being undertaken at the bilateral and regional/subregional level? How can the OEWG facilitate the sharing of good practices that can be applied at the global level?**

Learn from and build on existing capacity-building efforts

There are numerous efforts under way when it comes to cybersecurity capacity building and there is likely no single entity that connects all of them. Microsoft has long supported various cybersecurity capability building initiatives and we would like to take this opportunity to highlight some of the efforts that we are actively participating in:

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- **Partnering with the United States Telecommunications Training Institute (USTTI):** Microsoft has helped the USTTI deliver training that equips officials from emerging economies with the skills needed to manage their spectrum, deploy wireless technologies, develop national broadband plans, implement national cybersecurity strategies, support Internet deployment, launch cloud services, protect children online, and ensure sound emergency communications plans all while working to support the rule of law.
- **Supporting the Global Forum on Cyber Expertise (GFCE):** Microsoft has supported the GFCE since its inception and continues to be an active participant in its working groups. In addition, we have supported the creation of the GFCE-Microsoft Africa program fellowship, which focuses on mapping,and ultimately streamlining existing cybersecurity capacity building efforts in Africa.
- **Working to deliver sound national cybersecurity practices through the International Telecommunications Union (ITU):** Microsoft has been a core partner to the ITU in developing a "National Cybersecurity Strategy Guide[24]" and we have continued to support efforts to ensure its effective implementation around the world.
- **Identifying opportunities across Latin America***:* Microsoft has for a number of years partnered with the Organization of American States (OAS)[25] to promote good practices, in particular as it relates to critical infrastructure protection and addressing cybercrime.
- **Supporting international IoT cybersecurity standards with the Internet Governance Forum (IGF):** Microsoft is a partner and participant in the IGF Dynamic Coalition on Internet Standards, Security and Safety. The Dynamic Coalition is focused on increasing the adoption of international standards by facilitating access to best practice recommendations.

We particularly encourage the OEWG to build on the work done by the Global Forum on Cyber Expertise (GFCE) as a donor coordinator given its existing function on capacity building and community efforts. The GFCE could be leveraged, or used as model to coordinate assistance initiatives through a system for matching needs and resources. This would help build momentum and avoid duplication of efforts.

2. How can the OEWG facilitate the mapping of existing needs for better coordination and resourcing of capacity-building efforts? Can the UN play a matchmaking or repository role in capacity building?

Leverage the match-making capabilities of other stakeholders

Even with increased attention on cybersecurity capacity building, the supply of such initiatives continues to fall well short of demand. Well-coordinated international efforts are critical to ensuring at least a common baseline level of cyber resilience and understanding across the globe. Therefore, rather than duplicate the matchmaking function of such entities as the CyberPeace Institute[26] or the GFCE we encourage the OEWG, and the UN by extension, to build on existing initiatives and explore effective partnerships with them. We highlight these types of initiatives in particular because they are multistakeholder in nature. We are concerned that any effort that the UN would pull together would by definition look to States alone. With that in mind, we encourage all States to actively participate in those efforts – either in the recipient or donor capacity.

3. What are other aspects the OEWG should consider with regard to this topic?

[24] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

[25] https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-009/18

[26] https://cyberpeaceinstitute.org/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

Build on existing initiatives, understand underlying needs and leverage the multistakeholder community

Building on the outcomes of the previous OEWG and GGEs, this current OEWG has the potential to positively impact the security and stability of cyberspace by promoting cybersecurity capacity building to a broader audience. Over the past decade, cyberspace has become an intrinsic part of the development of any country. However, while technology creates untold opportunities and enables everything from distance learning, to groundbreaking innovation and new economic efficiencies, it also introduces new threats. As such, a strong understanding of cybersecurity good practices is crucial for States' abilities to benefit from the potential that technology offers. Moreover, the interconnectivity of cyberspace means that it is in the interest of all states to increase the preparedness of all relevant stakeholders – in a networked world, we can only be as secure as our weakest link.

In broad terms, cybersecurity capacity building is focused on building functioning and accountable institutions that can respond to threats emanating from cyberspace, enhancing States' overall cybersecurity resilience, and equipping stakeholders to be able to participate in international debates on cybersecurity to implement the decisions taken. International law, norms, and confidence building measures can only be implemented and adhered to if States have the capacity to act on them. This is why we have in recent years seen a greater focus on cybersecurity capacity building by civil society, industry, and governments around the world. This means mainstreaming cybersecurity capacity building efforts into the broader development agenda, as exemplified by the Sustainable Development Goals.

With that in mind, Microsoft reiterates its position on these issues and encourages States to:

- **Utilize existing mechanisms.** Numerous entities have dedicated funding and resources to capacity building initiatives. Instead of replicating those efforts, Microsoft encourages States to pool resources to generate greater impact, and participate in fora, such as the Global Forum on Cyber Expertise, which can help match needs with expertise.
- **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 an understanding of where they have gaps in capacity or capability. Inevitably, these needs will vary depending on regional or local context.
- **Strengthen cybersecurity diplomacy.** All too often, cybersecurity capacity building efforts focus on the technical aspects of cybersecurity — which are necessary, but not sufficient. One area that would benefit from additional capacity building attention and resources are efforts to strengthen cybersecurity diplomacy capabilities in countries around the world. The Cybersecurity Tech Accord has recently published a paper on this topic: Effective Cyber Diplomacy White Paper: A Guide to Countries' Engagement in International Security Dialogues[27]. Efforts such as these would help to ensure that all States are equipped to participate in relevant international negotiations on a more equal footing and ensure we make further progress.
- **Be inclusive of all stakeholders.** It is critical that capacity building focuses not just on government stakeholders, but industry and civil society as well. This means both ensuring that the different stakeholder groups are trained on cybersecurity, but also that they their viewpoints are considered when trainings are developed. Furthermore, they can often help scale and address cybersecurity needs. For example, Microsoft recently launched[28] national campaign in the United States to help community colleges expand the cybersecurity workforce. Partnerships such as this one can drive a whole of society approach to cybersecurity and truly make a difference.

[27] https://cybertechaccord.org/effective-cyber-diplomacy-white-paper-a-guide-to-countries-engagement-in-international-security-dialogues/

[28] https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- **Safeguard and promote human rights.** A global, open, free, accessible, stable and secure cyberspace, where individuals' internationally recognized human rights are protected and respected, is essential for the inclusive sustainability, development and security of all societies. These universal values need to be part of all cybersecurity capacity building efforts.
- **Maintain relevance and ensure sustainability**. Technology is evolving rapidly, and it is important to ensure that capacity building efforts are outcome-focused. Capacity building needs to be treated as a continuous process with near- and long-term objectives, rather than a one-off engagement.

Establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States

1. In the long-term, how can a future regular institutional dialogue support action oriented measures in view of the evolving peace and security threats posed by State use of ICTs?

Establish a permanent UN forum, open to meaningful input from all stakeholders

Microsoft has closely followed and provided input as able to various UN initiatives and dialogues on cybersecurity over the past two decades. This includes the previous OEWG, as well as the multiple iterations of the UN GGE. Unfortunately, despite the progress that has resulted from these dialogues in building an international framework for peace and stability in cyberspace, the overall security of the online environment has continued to deteriorate. The number of countries investing in offensive cyber capabilities has continued to increase, and attacks have grown more frequent and more sophisticated, in apparent disregard of international expectations. Incidents like Nobelium (SolarWinds) and Hafnium (Microsoft Exchange) attacks illustrate just how far governments are willing to go in targeting their adversaries, irrespective of whether civilians might be caught in the crossfire.

Against this backdrop, we believe that more needs to be done at the international level to achieve real progress in increasing the security and stability of cyberspace. In particular, there needs to be a regular and ongoing dialogue amongst all interested parties on these critical issues. The current trends do not inspire confidence that the issues we face will go away in the foreseeable future, and in fact the past two decades teach us that as technology evolves, so will offensive techniques. A permanent discussion forum is therefore urgently needed, and will go some way to ensure that the process is not captured by geopolitical interests. Moreover, the distinct lack of meaningful and systematic multistakeholder inclusion in these debates needs to be urgently addressed.

We believe the proposed Programme of Action (PoA)[29] can be seen as a potential key step forward in this regard, and we strongly recommend States engage in a genuine dialogue that would see it it adopted, ideally sooner rather than later. At the same time, we note that as the PoA is envisioned as a permanent body that is expected to navigate a field that values speed and innovation, it is critical that it retains the flexibility for states to agree on new areas of work over time. The original proposal already highlights the possibility of States submitting working papers on specific thematic issues, but we believe that if the PoA wants to remain true to its commitment to working with the multistakeholder community, it must go a step further. As such, we encourage States to consult amongst each other, and with the multistakeholder community, on an annual basis to determine whether existing areas of priority remain relevant and whether new areas of work should be introduced. This should include the ability for non-governmental participants to propose new areas of action.

[29] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf