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

Microsoft

Microsoft's submission to the Open-Ended Working Group on security of and in the use of information and communications technologies

December 2022

Microsoft welcomes the opportunity to provide our submission to the informal inter-sessional meeting of the Open-Ended Working Group on the security of, and in the use of, information and communications technologies (OEWG). This submission addresses the questions posed by the Chair in his November 22 letter, and provides additional details to the statements we delivered in the December inter-sessional meeting. We want to express our gratitude to the Chair for his flexibility and efforts to include participants from across the multistakeholder community to inform OEWG deliberations.

We hope our input proves useful and we remain ready to offer additional contributions.

THEMATIC SESSION: GLOBAL POC DIRECTORY

1. *Will the directory be available via webpage (publicly available webpage or by password-protected webpage for States only), by periodic circulation via email or through other means of dissemination? What are the advantages and disadvantages of each of these modes of dissemination?*

   There is value in making this information publicly available and as accessible as possible. Microsoft therefore encourages this information to be maintained on a public website. While we understand that the primary reason for this directory should be to improve communication between and among states, there may be occasions where members of the multistakeholder community want or need to share pertinent information with a particular state as well. Having an easily accessible point of contact directory could significantly expedite and improve those exchanges. This website could, for example, be maintained by the United Nations Office for Disarmament Affairs (UNODA) on their domain.

2. *How many POCs should each State nominate – for example, distinct nominations for the diplomatic and technical levels? How can the nomination of global POCs be coordinated with the work of POCs at relevant regional directories and CERT organisations to build on already existing channels of communications and to avoid duplication?*

   Microsoft believes states should nominate a single POC - with a backup - and that this individual is given the responsibility of navigating the various national structures in response to requests. States organize their cybersecurity governance quite differently and it would therefore be impossible to mandate the same organization with responsibility for this area across all states. The most effective way to identify the appropriate organization to follow up on a request is to place this responsibility with states to designate a single point of contact.

   In general, we would recommend that the POC comes from either the diplomatic corps or from an entity dealing with cybersecurity at a strategic level to avoid duplication with existing efforts, which have typically focused on operational and technical considerations. In particular, we would strongly recommend working with the Forum of Incident Response and Security Teams (FIRST)[1] on technical

[1] https://www.first.org/about/

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

POCs. FIRST has over years built a strong and active community of national CERTs and other technical teams, which the OEWG should not seek to duplicate or emulate, but should instead leverage.

3. *What information should be provided for each of these POCs? (e.g. Name, title/position, email, phone, preferred UN languages, availability etc.)*

   Based on our experience in working in information sharing organizations, Microsoft recommends that the information provided for the POCs includes their name, position, contact details and date when it was last updated. We consider the question of designating preferred UN languages a nice-to-have, but also a potential barrier to cooperation, as we can easily envisage a situation where individuals would be unwilling to reach out to a particular POC if they do not attest to speaking their preferred language. As such, we recommend that nominated POC, at a minimum, are able to communicate in English.

   Finally, it is our experience that a generic email address, which several people can access, is helpful to avoid situations when the primary POC is unable to respond (e.g., due to vacations, illness etc.).

4. *How often should POC information be updated and by what means?*

   Microsoft suggests that the directory is systematically reviewed on an annual basis by the entity that will host it, such as, for example, UNODA. Of course, that would not preclude states from communicating any changes or updates to the responsible entity as soon as these occur. In line with the above, we recommend these updates are implemented by a single centralized entity and that any changes are communicated over email to ensure there is no miscommunication and that a written record of the exchange exists.

5. *What measures can be put in place to ensure that the information in the directory is accurate and updated? (e.g., periodic "ping" tests conducted by the directory manager)*

   Please see the answer to question 4.

6. *How could capacity-building initiatives be utilized to assist States in identifying and equipping POCs and also to make use of the global directory?*

   It can be anticipated that the use of the global directory will evolve over time. However, at this early stage we believe that its primary value would be a combination of acting as a Confidence Building Measure (CBM) in and of itself, and as a vehicle for implementation of other CBMs at the global level. As one example, cybersecurity exercises and trainings relating to the implementation and operationalization of the global directory would both build capacity and understanding of the benefits of the directory, as well as contribute to building trust amongst states. With that in mind, we would recommend the entity responsible for maintaining the directory organizes such an exercise, at a minimum, on a bi-annual basis.

   As the use of the directory expands over time, for example to incorporate reporting of incidents or threat information, capacity building efforts being made available to the community should evolve also.

7. *What policies (if any) shall govern communication between POCs? What lessons or models can be drawn from other POC directories such as at the regional level and CERT organisations?*

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

Microsoft encourages states to share as much information as possible publicly – eventually. However, it is important to recognize that any communication during a crisis, or reporting of incidents, for example, needs to be confidential. The confidentiality of information will also be increasingly important if states expand the use of the directory to complement and strengthen existing international and regional Computer Security Incident Response Team (CSIRT) POC arrangements for the operational and technical exchange of cybersecurity threat and cyberattack-related information.

For these circumstances, we would recommend leveraging international standards that guide coordinated vulnerability disclosure[2] and that have been leveraged for both threat and vulnerability information sharing by CSIRT and private sector players around the world. At the heart of those guidelines is the requirement to only share information with those who need it to be able to resolve the situation – not only states, but private sector actors in particular.

8. *Should there be a distinction between working-level and senior-level POCs? If a distinction is made, under what circumstances may senior-level POCs be contacted?*

   To ensure the process is as streamlined as possible, Microsoft recommends states put forward a working-level individual at the POC and retain the ability to escalate internally, as they see fit. In addition, based on our experience of working within different trade associations or within information exchange programs, we would recommend that each state puts forward a contact alias email that goes to several individuals to ensure that someone is always reachable, even if the primary POC is unavailable.

9. *What policies, protocols and processes (if any) should govern the exchange of information among POCs? Can information exchanged be shared with inter alia (a) other States, (b) other non-State entities, or (c) made publicly available?*

   Please see the answer to question 7.

10. *What additional activities could be pursued to leverage the expertise available within the POC directory with the view of building on existing regional POC directories and CERT-to-CERT arrangements? (e.g., table-top exercises, information exchange mechanisms between policy makers and the technical community, incident response procedure?)*

    Microsoft is enthusiastic about states taking concrete and practical steps towards operationalizing the international framework for responsible state behavior in cyberspace. We therefore welcome the POC directory, as it would, in our opinion, not only build confidence between and among states, but also serve as a tool to pursue other cooperative measures to address threats arising from malicious use of such technologies. We would encourage states to be as ambitious as possible in defining this function. It could serve as a foundation for a vibrant global network of cybersecurity policymakers and practitioners to:

    - Facilitate information-sharing around latest threats, and possible mitigation measures;
    - Support de-escalation and coordination in the face of major ICT incidents;
    - Promote trust-building within the community, including through regularized exchanges.

[2] https://www.iso.org/standard/72311.html and https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

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

Microsoft

THEMATIC SESSION: CONFIDENCE-BUILDING MEASURES

1. *What concrete, specific CBMs are currently in place at the (sub-)regional level in the ICT security domain that could be expanded to the global, inter-governmental context?*

   Microsoft recognizes the importance of Confidence-Building Measures (CBMs) as tools to reduce tension, minimize the risk of misperception, and build trust. CBMs can act as a pressure valve and can therefore help deescalate critical situations. It is worth noting that, to a certain extent, a mechanism such as the OEWG constitutes a CBM in and of itself.

   When it comes to examples of other specific CBMs, Microsoft would direct the OEWG's attention to research conducted by the Global Forum for Cybersecurity Expertise (GFCE)[3]. The Task Force on CBMs, Norms Implementation and Cyber Diplomacy in 2020 developed an overview of existing CBMs for cybersecurity and made it publicly available[4]. Many of the examples included in the document could be replicated in their entirety at the international level. Alternatively, approaches used in regional conversations could be leveraged to develop similar approaches with a great number of participants.

   However, rather than focusing on any specific new measure, we would urge the OEWG to encourage more active participation in the implementation of the CBMs agreed to as part of the UN Group of Governmental Experts on information security in 2013 and 2015[5]. Specifically, we would like to see:

   - voluntary sharing of views on international law and its applicability to cyberspace;
   - voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations related to security of and in the use of ICTs as well as the procedures for this sharing of information;
   - voluntary sharing of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term.

2. *Are there concrete, specific CBMs currently in place within other domains in the field of international security that could be adapted to the domain of ICT security?*

   There are numerous CBMs from the conventional arms domains that states have already sought to introduce to cyberspace, and that Microsoft believes should be emphasized further. These, amongst others, include:

   - Organizing seminars and workshops with the aim of promoting transparency and dialogue. Microsoft believes that in effective implementation of cybersecurity CBMs states should rely on the experience and expertise of all relevant stakeholders. As such, we propose to also invite representatives from the multistakeholder community to take part in these seminars.
   - Promoting dialogue, as appropriate, and on the basis of mutually agreed parameters, on strategies and policies governing the use, deployment, control as well as trade and transfer of conventional weapons. We believe that in the cybersecurity domain, states should in particular discuss their vulnerability equities policies. By providing greater transparency around how governments decide to handle a vulnerability – whether to retain it to be exploited or to disclose it to a vendor to be fixed - states will be less inclined to assume worst intentions.

[3] https://thegfce.org/

[4] https://cybilportal.org/wp-content/uploads/2020/05/GFCE-CBMs-final.pdf

[5] Ibid

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

- Preventing, combating and eradicating the diversion of conventional weapons into the illicit market or to criminals, illegal armed groups, terrorists or other unauthorized recipients. Here, Microsoft calls on states to begin discussing how to limit the transfer of cyberweapons to criminals, as well as how to counter or, at a minimum, put limits on the emerging cyber mercenary market[6].

3. *Recommendation 5 under Section E (Confidence-Building Measures) of the OEWG's first Annual Progress Report (APR) encouraged States to continue, on a voluntary basis, to share information through the report of the Secretary-General on developments in the field of ICTs in the context of international security, as well as the UNIDIR Cyber Policy portal as appropriate. What further measures (if any) can be taken by States and/or the OEWG to better utilise existing resources and platforms to promote increased confidence and transparency between States?*

   Microsoft believes that the OEWG can provide a "forcing function" for states to act, implement and publicly report on their transparency measures and lessons learned. We reiterate that the OEWG could incentivize states to make use of the of the online self-assessment tool for a National Survey of Implementation of United Nations recommendations on responsible use of ICTs by states in the context of international security, as proposed by Australia, Mexico and others[7], to also include their CBM-related efforts when they submit their responses. As proposed in our previous submissions, the Chair could encourage states to report on their deliverables on an annual basis, which would create a deadline for them to meet, and thereby hold states accountable. This, in and of itself, would also represent a CBM.

   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 these CBM-related commitments. It is our experience that having a Secretariat is the most effective way to ensure regular reporting and capture most up to date information.

4. *Are there any concrete, specific initiatives which other interested parties, including businesses, non-governmental organizations and academia, could independently develop and implement that could contribute to confidence-building between States? (e.g., voluntary information sharing initiatives)*

   Trust and confidence between states, to serve as the basis for cooperation, requires recognition of a shared set of facts. It is hard to build trust when states disagree or simply don't collectively recognize the same challenges in a domain. This can be especially difficult when it comes to cyberspace, where the risks and attacks can remain hidden. The technology industry – broadly speaking – can uniquely support a shared understanding among states of the threat landscape and priority issues online by explaining the trends and challenges respective companies are identifying. While each technology company has a limited view of cyberspace, in aggregate their insights can highlight the most pressing issues. To this end, the Cybersecurity Tech Accord – a coalition of more than 150 global technology companies – is launching a quarterly newsletter, "Required Update," capturing threat intelligence reports and other information from across the industry for the benefit of the growing community of diplomats focused on cybersecurity and other tech policy issues. We would encourage OEWG representatives to info@cybertechaccord.org, to be added to the list of recipients.

---

[6] https://www.ohchr.org/sites/default/files/Documents/Issues/Mercenaries/WG/CyberMercenaries/MSFT-Response.pdf

[7] https://www.internationalcybertech.gov.au/sites/default/files/2020-12/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf

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

THEMATIC SESSION: (A) EXISTING AND POTENTIAL THREATS, AND (B) RULES, NORMS AND PRINCIPLES OF RESPOSNIBLE STATE BEHAVIOUR

1. *Paragraph 11 of the Annual Progress Report refers to new and emerging technologies whose properties and characteristics can create "new vectors and vulnerabilities that can be exploited for malicious ICT activity". What are these new and emerging technologies and how are they exploited for malicious ICT activity? How can the international community collectively develop a deeper understanding of their potential risks?*

   Microsoft urges the OEWG to not necessarily think about new and emerging technologies as potentially "game changing" breakthroughs for security. While this might be the case with some innovations -- for example those in quantum computing or artificial intelligence (AI) -- dramatic changes can also emerge from adapting existing technologies to new uses – such as creating new opportunities to leverage it for criminal purposes or adapting it to new environments. One such example is the increasing use of technology across critical infrastructure sectors. Specifically, while leveraging technology in hospitals has driven significant advances in patient care, it has also exposed hospitals to new cyber risk, including increasing ransomware attacks.

   To develop a deeper understanding of these issues, we recommend the OEWG engages with the private sector, academia, and the technical community on a regular basis. Specific thematic briefings would allow for a greater exploration of particular technologies, their potential use and abuses, as well as consideration of potential guardrails that might be put in place.

   We have attached our proposals on AI and cybersecurity to this submission.

2. *What concrete, specific initiatives can States and other interested parties undertake within the framework of the OEWG to mitigate the impact of new and emerging ICT threats on international security?*

   Our collective efforts should prioritize (a) understanding the threat landscape, (b) implementing agreed upon measures/holding violators accountable, (c) strengthening the framework by providing additional guidance, and (d) identifying gaps in the framework and responding to changes in the threat landscape. With that in mind, we suggest states act in several priority areas:

   - First – we call on states to secure global ICT supply chains from evolving threats by prohibiting cyberattacks on ICT supply chains, especially those targeting software and security update mechanisms. Such attacks cannot be seen as targeted and are by definition indiscriminate, and therefore fundamentally inconsistent with responsible state behavior. They undermine trust and security in the entire digital ecosystem and should clearly be seen as off limits.
   - Second – we urge states to take further steps to protect critical infrastructure. To this end, we welcome the call for specific measures to safeguard the '*public core*' of the internet. As practical next steps, we encourage states to keep defining specific components of critical infrastructure essential to the internet's functioning. In particular, the OEWG could (a) recognize the growing ICT threats against physical infrastructure, such as underseas cables, which perform key functions in delivering internet services regionally or globally and (b) make such attacks off limit.
   - Third – we recommend states take further steps to protect humanitarian organizations from cyber harm: Protecting humanitarian organizations and the data they hold, as evidenced in the attack on the International Committee of the Red Cross (ICRC) last year, is critical. We call on states to affirm that humanitarian organizations provide critical services and should be off limits to cyber harm, in both times of war and peace.

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

- Fourth, we urge states to limit the use of cyber mercenaries. This rapidly expanding industry profits from developing and selling tools, techniques, and services to allow their clients to break into ICT networks and devices. This practice undermines trust and security in the online environment, gravely impacts human rights, and violates the spirit of norm '(j)' in the 2015 GGE report. This norm calls on states to encourage responsible reporting of ICT vulnerabilities rather than enable, within their jurisdiction, their stockpiling and exploitation for profit.

We have attached our detailed proposals to this submission.

3. *Which technical developments have States identified as contributing to emerging and potential threats, inter alia those referenced in paragraphs 8 to 13? (e.g., proliferation of marketplaces for zero-day exploits, systemic effects of vulnerabilities in widely used open-source software). What further measures can be undertaken by States to reduce the risk to international security posed by such developments?*

While it is important to recognize new risks posed by emerging and potential threats – including threats to open-source software (OSS) and the proliferation of ransomware attacks – the commitments states can make to mitigate these threats are largely consistent with established best practices. The number of states that have adopted publicly available vulnerability equities processes (VEP) remains well below the number of states that have offensive cyber programs. VEPs should be a prerequisite for having such programs and make clear that systemic vulnerabilities, such as those in OSS should *always* be immediately disclosed and never purchased to be exploited. States should also make clear commitments to never employ or condone the use of ransomware, as such attacks could never be consistent with responsible state behavior.

4. *In light of existing and potential threats identified by States, including those referenced in the APR, what specific capacities would States require to (a) support implementation of the framework for responsible State behaviour in the use of ICTs; and/or (b) develop of an adequate security infrastructure to mitigate these threats in ICT security?*

Please note our responses in the capacity building section that follows.

5. *Are there any suggestions for updates or further elaboration to the non-exhaustive list of proposals annexed to the Chair's Summary in the 2021 OEWG Report, in light of further discussions that have taken place within the OEWG since then?*

    - *Which of these proposals ought to be developed further so as to be incorporated into future Annual Progress Reports of the OEWG?*
    - *What can be done to help facilitate a deeper discussion on these proposals so as to achieve the potential attainment of consensus on some or all of these?*

As highlighted in other areas of this submission, Microsoft believes a number of the original proposals should be elaborated upon or updated further to reflect the changes in the external environment, as well as to advance the implementation of the existing framework. These, inter alia, include:

- Elaboration of the normative framework, as highlighted in our response to question two of this section. A number of states put forward proposals around critical infrastructure protection, and Microsoft supports further work in this area. In addition, we align ourselves with the Dutch

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

proposals on the public core and election security and wish to highlight these as a matter of some priority.

- Additional focus on international law, in particular as it relates to the international humanitarian law in light of the novel use of offensive technologies in Ukraine. Please note our response in the international law section of this submission;
- Closer work with the multistakeholder community across the discussions in the OEWG, but particularly on threats, as elaborated in answer 1 of this section.

We encourage the OEWG to prioritize a small number of concrete proposals in the coming year and organize dedicated sessions that would allow these to be examined in some detail. Those discussions would also reveal what the "red lines" are for states and where progress could potentially be made.

6. *Which topics should be most urgently examined in the context of developing guidance and/or checklists so as to facilitate developing common understandings on rules, norms and principles of responsible State behaviour in the use of ICTs?*

   Please note our response to question 2.

7. *Can and should member states continue to share national views on additional norms that could continue to be developed over time, particularly in the context of the evolving cyber landscape and ICT security environment?*

   Microsoft strongly supports this proposal. We believe there is scope for both development of additional norms, as well as elaboration of current norms with more specific examples and clarifications of obligations and prohibitions. The attachments we have submitted together with this response retain specific proposals that we hope would be considered by states.

8. *What are some of the basic capacities required to implement the framework for responsible State behaviour? How can States be supported in the acquisition of those capacities?*

   Please note our responses in the capacity building section that follows. We want to particularly highlight the importance of states exchanging experiences when it comes to implementation of the framework, both as confidence and capacity building measures. With that in mind, we hope that states proactively share how they are implementing the framework both at the OEWG and on the United Nations Institute for Disarmament and Research (UNIDIR) cyber portal[8].

[8] https://cyberpolicyportal.org/

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

Microsoft

THEMATIC SESSION: CAPACITY-BUILDING

1. *How can the principles of capacity-building in relation to State use of ICTs in the context of international security as adopted in the 2021 OEWG report be integrated into international and regional capacity-building efforts?*

   The principles adopted in the 2021 OEWG report are, to a large extent, already integrated into well-established capacity building efforts, in particular those that seek to address multiple countries at the same time. Nevertheless, we would recommend that the OEWG continues to promote these principles to states, as well as to other potential donors in the multistakeholder community, to raise awareness, avoid duplication and ensure they are incorporated into their funding commitments.

   This could be done by organizing a dedicated session focused on cybersecurity capacity building as part of the OEWG considerations. The session could explore the principles and their importance for implementation of capacity building efforts and target in particular the various implementors. It could also serve as a match-making exercise, highlighting both funding and training opportunities available. It is worth noting that this type of capacity building can also build trust and confidence. As such, the OEWG would have an opportunity to be a nexus for both capacity-, and confidence-building.

2. *Are there concrete, specific capacity-building mechanisms currently in use at the (sub) regional level in the ICT security domain that could potentially be expanded to the global, inter-governmental context?*

   Microsoft has observed numerous (sub) regional initiatives dedicated to cybersecurity capacity building that have a proven track record and have successfully supported particular states with improving their cybersecurity posture. The work of the Organization of the American States (OAS)[9] or the ASEAN-Singapore Center of Excellence[10] is worth highlighting in particular.

   Nevertheless, we would caution against expanding these efforts to a global context without further thought and investigation, as well as a mapping of existing efforts to avoid duplication. While some of the approaches utilized are easily transferable, a key part of the success of these initiatives comes from taking local considerations into account, as well as from using these efforts to build a supportive and relatively localized community. At this stage it might be worthwhile to highlight what we believe are crucial considerations and responsible practices in cybersecurity capacity building:

   - *Understand the need.* Capacity building efforts can only succeed if they respond to a real need in a targeted way. 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.
   - *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, social, judicial, … etc. This is neither effective nor sufficient, especially in the long term.
   - *Be culturally responsive and ensure initiatives are locally owned.* While users world-wide increasingly connect to the same public Internet, the ways in which they use modern technology and learn new information is heavily influenced by local customs and cultures.

[9] https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

[10] https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence

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

- *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.
- *Be inclusive of all stakeholders.* It is critical that capacity building focuses not just on government stakeholders, but industry and civil society as well. All of these stakeholders must be involved in the design, development and delivery of capacity building programs.
- *Incorporate human rights.* A global, open, free, accessible, stable and secure cyberspace, where human rights and fundamental freedom apply, is essential for the well-being, growth and prosperity of all societies. These core values need to be part of any cybersecurity capacity building efforts.

3. *Are there concrete, specific capacity-building mechanisms currently in use within other UN fora that could potentially be adapted to the ICT security domain?*

   UNIDIR's Cyber Policy Portal[11] is a noteworthy example in this regard. In many ways it represents both a capacity-building mechanism as well as a confidence building measure.

4. *Are there existing funding mechanisms that could be leveraged for capacity-building in the area of security of and in the use of ICTs? How can the States and the OEWG work together with those development programmes and funds to unlock greater access to capacity-building for developing countries?*

   Threats emanating from cyberspace continue to be a significant threat for governments, organizations and individuals around the world. From supply chain disruptions to ransomware attacks, cybercriminals have become increasingly sophisticated and the threat landscape more diverse, dispersed and dangerous. These threats are compounded by a workforce shortage; there simply aren't enough people with the cybersecurity skills needed to fill open jobs. This is a global problem. Some estimate that by 2025 there will be 3.5 million cybersecurity jobs open globally, representing a 350% increase over an eight-year period[12] and exacerbating an already massive cybersecurity skills gap.

   Unfortunately, despite this clear need, while there are some funding mechanisms available for cybersecurity capacity building, the demand far exceeds supplies. Moreover, much of the available funding is fragmented, spread across different states, global foundations and the private sector. As a result, potential recipients often aren't aware of available funding opportunities or how to access them. The one exception here is the World Bank's Cybersecurity Multi-Donor Trust Fund[13], a welcome effort to pool resources and ensure that limited funds stretch further.

   The OEWG could play an important role in changing the current status quo. For example, it could seek to generate political will behind cybersecurity capacity building. The International Chamber of Commerce recently put forward the idea of Cyber Development Goals, a call to action to motivate states to implement agreed upon norms on a specific timeline, supported by funding and other capacity building resources. We believe an initiative like this would not only motivate states to do more to implement the existing cybersecurity frameworks, but also help mobilize donor commitments. Here, the OEWG could be particularly helpful in working with states and various UN institutions to organize a

[11] https://cyberpolicyportal.org/

[12] https://cybersecurityventures.com/jobs/

[13] https://www.worldbank.org/en/programs/cybersecurity-trust-fund

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

cybersecurity capacity building donor conference, seeking to increase and more efficiently distribute the amounts of funding currently dedicated to this pivotal effort.

5. *How can the OEWG best leverage existing capacity-building initiatives in the area of security of and in the use of ICTs? What are the potential opportunities for synergy and coordination among existing initiatives? Are there gaps that need addressing?*

   Microsoft believes that it is important that the OEWG does not seek to replicate the solid cybersecurity capacity building work that is already being done across the various forums and initiatives. The OEWG should instead map existing resources and ensure that states and the multistakeholder community can access them easily. We recommend the OEWG work with the GFCE as part of this workstream. The latter aims to provide a matchmaking service between donors, implementors and recipients and is therefore already plugged into many existing efforts.

   Furthermore, the OEWG can also lead various UN agencies, regional organizations, and multistakeholder platforms to implement the capacity building principles introduced in the 2021 OEWG final report[14]. It can work to periodically review progress made – initially by encouraging states to fill in the self-assessment tool of the national survey originally proposed by Australia and Mexico, which is currently available on the UNIDIR's Cyber Policy Portal[15].

   Finally, cybersecurity capacity building would benefit greatly from being more closely incorporated and "mainstreamed" into broader, existing development efforts. While we recognize that cybersecurity issues touch on international peace and security, as well as national security, we nevertheless firmly believe cybersecurity should not be an add on, but a core element of digital transformation. With that in mind, we urge the OEWG to explore ways to connect these efforts with other development workstreams at the UN and beyond.

6. *Are there good practice examples of public-private partnerships on capacity-building in the area of security of and in the use of ICTs? Are there lessons that can be gleaned from those examples?*

   Serious efforts to improve cybersecurity capacities will require meaningful involvement of and cooperation with the multistakeholder community. Industry, civil society, and academia are already taking part in capacity-building initiatives; from implementing norms and driving cyber hygiene to providing clarity on applying international law in cyberspace and developing incident response plans and procedures for protecting critical infrastructure. In fact, we would be hard-pressed to find examples of capacity building where stakeholders either have not or could not add value.

   There are numerous examples of public private partnerships in particular that are worth highlighting, many of them driving implementation of cybersecurity norms at national levels. However, specifically related to the OEWG, examples of how Microsoft has engaged in capacity building in the past include:

   - Sharing high level threat information and our assessments of the latest trends with the international community as part of our commitment to transparency and protecting the digital ecosystem.
   - Developing a second edition of the ITU National Cybersecurity Strategy Guide and materials[16].

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

[15] https://cyberpolicyportal.org/

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

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

- Supporting the CyberPeace Institute's CyberPeace Builders[17] program, which works to increase the resilience of non-profits around the world through a corporate network of volunteers.
- Contributing to the GFCE, including by chairing the GFCE's international cybersecurity norms workstream, and supporting the establishment of GFCE CCB Coordination Committee for Africa.
- Participating in the U.S. Telecommunications Training Institute (USTTI)[18] capacity building program, with dedicated workshops on cloud security and cybersecurity policy.
- Promoting critical infrastructure protection, including by working on good practices compendia with civil society partners and the governments of Slovenia, the Czech Republic and Canada, on topics such as critical infrastructure protection, healthcare cybersecurity and election security[19].

7. *How can States raise awareness of the gender dimensions of security of and in the use of ICTs and promote gender-sensitive capacity-building at the policy level as well as in the selection and operationalization of relevant projects?*

   Not only states, but the multistakeholder community as a whole should take gender into account when it comes to cybersecurity capacity building. The focus on gender is important to retain across policy development and operationalization of specific projects, but also when it comes to recruitment. The global cybersecurity workforce is woefully lacking in diversity: on average, only 17% of the cybersecurity workforce are female.[20] Leaving women out of the cybersecurity workforce not only leaves talent on the table, but also makes it difficult to ensure that the policies we are developing take gender into account.

   Initiatives such as the Women in International Security and Cyberspace Fellowship (WIC)[21] that aims to address the need for a greater proportion of representation from women at the UN negotiations concerning cyberspace, go some way towards addressing this challenge. However, in addition to the workstreams that are focused specifically on the work of the OEWG, the global community should do more to break down the gender divide in this field.

   Microsoft has made women a priority for our cybersecurity skilling programs. For example, we have launched a partnership with Women in Cybersecurity[22], a nonprofit with the mission of recruiting, retaining and advancing women in cybersecurity, to expand their student chapters across 23 countries, helping promote the retention and advancement of women in cybersecurity. Additionally, in India we have since 2018 helped young women with mentoring from industry experts, especially from women leaders in the field, followed by job placement assistance with leading companies through our CyberShikshaa program[23]. In addition to initiatives that seek to increase the percentage of women in the cybersecurity workforce overall, we have also adopted a number of practices that have ensured that in 2022 women made up more than 30% of the Microsoft's core workforce worldwide.

---

[17] https://www.cyberpeaceinstitute.org/cyberpeacebuilders

[18] https://ustti.org/about-ustti/

[19] https://blogs.microsoft.com/eupolicy/2022/07/28/protecting-critical-infrastructure-from-cyberattacks/

[20] Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries - The Official Microsoft Blog

[21] https://thegfce.org/women-in-international-security-and-cyberspace-fellowship/

[22] https://www.wicys.org/

[23] https://www.dsci.in/cyber-shikshaa/

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

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

Microsoft

THEMATIC SESSION: INTERNATIONAL LAW

1. *Which areas of international law and legal issues should States prioritise and how can these be examined with a view to moving towards greater convergence?*

   It is Microsoft's view that the question of application of international law to cyberspace is one that needs to be prioritized with some urgency. Four decades after the official birth of the internet and almost twenty years after attacks on Estonia put cyberwarfare on the map, it can no longer be claimed that cyberspace is a new domain of conflict. Given the speed of innovation in this field, the number of areas that could benefit from an in-depth investigation of what role international law plays in guiding state conduct in this domain has grown exponentially in the intervening period.

   However, given the limited time and resources available, we urge the OEWG to focus on topics that are timely and are therefore likely going to be of immediate utility to states. With that in mind, the OEWG should leverage the various analyses of the cybersecurity threat landscape that are available and identify trends that are likely to have an impact in the long run. For example, we would recommend the OEWG examine the (positive and negative) obligations states have when it comes to ransomware, artificial intelligence, or cyberattacks levied against healthcare providers, and even nuclear facilities. Even more pertinent, the war in Ukraine has provided an all-too-painful example of how cyber weapons are already being used in armed conflict. Clarifying the different responsibilities in cyberspace under international humanitarian law is therefore more urgent than ever.

   We would encourage the OEWG to deliver thematic briefings on these subjects, leveraging expertise that resides in entities such as the International Committee of the Red Cross[24] and the Oxford Process on International Law Protections in Cyberspace[25]. Furthermore, the OEWG should insist that states submit their own respective views on the topics identified regarding the obligations under international law in cyberspace.

2. *What are the existing legal frameworks that may be relevant to the regulation of States' conduct in cyberspace? Are there any gaps in such legal frameworks with regard to the regulation of States' conduct in cyberspace and if so, how should they be addressed?*

   Microsoft believes that international law in its entirety, including international human rights law and international humanitarian law, apply in cyberspace. However, we observe that because few states have gone beyond agreeing that these bodies of law apply to the online environment, there is uncertainty as to *how* they apply in practice. Moreover, states very rarely publicly outline whether they take international law into account when engaging in cyber activities, and remain similarly vague about what aspects of international law are breached when attributing offensive activities. This conduct gives rise to a perception that not only are there gaps in the existing framework that can easily be exploited, but also that by and large cyberspace is a lawless environment. This is a dangerous message to send, given continuously escalating threats emanating from cyberspace as a whole and, particularly, in light of the increasing incorporation of cyberattacks into armed conflict.

   To address this dangerous state of play, Microsoft encourages the OEWG to invite states to put forward statements on how they believe international law applies to cyberspace. A number of states have issued statements to that effect in recent years, and these have helped made clear how they view their roles

[24] https://www.icrc.org/en

[25] 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/

and responsibilities in the online environment. They have also helped identify areas where there might be convergence, as well as areas where there might be gaps. As more states contribute to this body of work, the international community can collectively build a greater understanding of how international law applies to cyberspace. The examination of different scenarios and problems, as proposed in the answer to the previous question, would have a similarly positive culminative effect.

Finally, Microsoft remains convinced that the more international law gets leveraged by states, the clearer and stronger the legal framework will become. As such, it is our hope that states will look to international law to guide their obligations in cyberspace, both when it comes to protection of the online environment and to exercising restraint, as well as in holding violators accountable.

3. *What types of capacities are needed to bolster States' understandings on how international law applies in the use of ICTs? How can we increase States' capacity thresholds in these areas, and to this end, what resources and institutional support, etc., are needed?*

At the outset it is important to underline that increasing states' capabilities in this area is a multifaceted challenge without a simple solution. Different states clearly have varying resources at their disposal, are at divergent stages of digital transformation, face distinct challenges in cyberspace, and therefore prioritize and understand these issues in very different ways. The result is thatthey have different needs in terms of bolstering their capacities and capabilities.

Nevertheless, all states have some things in common. They are all expected to be able to navigate a quickly evolving online environment, which includes understanding how the latest technologies can support their economic development and security posture, as well as comprehending the potential impact of associated threats. Frequently, much of this knowledge resides with the private sector and the companies that develop and operate these technologies. In addition, all states need to be able to traverse a very opaque field, where offensive capacities and capabilities are closely guarded secrets, and where a public dissection of a particular attack is an exception rather than the rule.

Microsoft therefore believes that this is an area that needs to be prioritized for systematic investments for the foreseeable future, since new areas will emerge as technology evolves and need examining through the lens of international law. We are further convinced that advances in this area can only be made by bringing together technologists, lawyers, diplomats, and national security experts in a true interdisciplinary fashion. While the foundation of the discussion might be international law, these other fields need to contribute to its interpretation and implementation.

Taking these constraints into account, we recommend a dedicated course is made available for all states and that it takes the form of scenario planning exercises. These could highlight specific examples of how technology has - or could be - used as part of offensive cyber operations and examine those with international law in mind. The course would not only build capacities but also contribute to confidence building between states, deepening understanding of how they view these different events. The OEWG could and should facilitate these types of exchanges between states, as we sorely need further awareness and alignment between states on this critical issue. However, we would also welcome greater focus on this area in regional bodies, such as the Organization of American States or the African Union. All these bodies would, however, be remiss if they closed their ears to some of the leading academic experts on international law. In recent years, it is academia that has driven clarity and understanding in this space. Whether we look at the efforts that delivered the Tallinn Manual or the more recent efforts by the Oxford Process on International Law Protections in Cyberspace, the knowledge and consensus built have significantly contributed to better understanding this thematic area.

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

THEMATIC SESSION: REGULAR INSTITUTIONAL DIALOGUE

1. *In considering regular institutional dialogue on the topic of ICT security within the UN, what are the key principles that need to be considered in their design? How do we ensure that discussions on ICT security at the UN continue in an inclusive manner, with the broad participation of all Member States?*

   The broad level of participation in the current OEWG by not only states, but – when possible – also the representatives of the multistakeholder community, demonstrates that there is an increasing awareness of the potential impact online threats can have – on the economy, on national security, as well as on individual rights and freedoms. We do not believe the expressed interest in and need to increase the stability and security of the online environment will diminish any time soon.

   Microsoft therefore urges states to ensure that any future dialogue is open to as many participants as possible. This should not include only states, but also relevant stakeholders from academia, civil society, and industry. Such an approach would reflect the reality that in developing solutions for the many challenges in cyberspace, states need to gather input and insights from those on the frontlines. Frequently, those bearing the brunt of the attacks are not government officials, but technical experts from the private sector.

   We also recommend that any future dialogue incorporates periodic reviews of the progress being made. We believe holding states accountable for existing and future commitments in this space will help increase participation, focus the discussions further, and in fact help drive implementation of the agreements. These reviews will, however, only be successful, if they are augmented with targeted funding or capacity building efforts to ensure a level playing field across the world.

   Microsoft has previously put forward a set of principles that we believe should be at the heart of any regular institutional dialogue on cybersecurity, and these incorporate the recommendations below:

   - provide practical support, including funding, for implementation of existing commitments;
   - build on existing agreements in the UN, but also incorporate effective international initiatives, such as the Paris Call for Trust and Security in Cyberspace[26];
   - incorporate robust human rights provisions;
   - ensure meaningful inclusion of all relevant stakeholders, including those from private sector, academia, and civil society;
   - retain sufficient flexibility to be able to respond to rapidly evolving digital threats.

2. *In considering the proposal for a Programme of Action with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, how do States understand its relationship with the OEWG? In what specific ways can the POA complement the ongoing work of the OEWG?*

   Microsoft believes that the Programme of Action (PoA) should be thought of as a separate mechanism and not a vehicle that grows out of the existing OEWG. In our opinion, the international community would benefit from and in fact urgently needs a permanent platform for regular dialogue on cybersecurity. As such, there is a need to acknowledge cyberspace as the 5th domain of conflict and the fact that associated challenges cannot and will not be resolved within current, temporary structures,

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

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

whose mandates need be re-negotiated every time they are set-up. Furthermore, it is important that any new process is not captured by any national or geopolitical interests. With that in mind, we were optimistic that an overwhelming majority of states (157) voted for the PoA resolution earlier this year and hope that even more support its establishment.

Against that background, we do not see the existing OEWG and a future PoA as being in competition, in particular as the PoA would only be set up after the conclusion of the current OEWG. In fact, we believe that the PoA could and should continue building on the progress made so far, not only in the current OEWG, but also across the previous UN processes on the topic. With that in mind, we urge states to consider the following areas of focus as priorities for the PoA:

- Implement agreed upon norms by developing conceptual and practical guidance on how the existing framework could be operationalized. For example, an early priority could be to encourage states to define what they consider critical infrastructure.
- Encourage stakeholders to regularly measure progress made on norm implementation. Technology will evolve as will the understanding on how to ensure stability and security of cyberspace. With that in mind the international community should ensure that implementation of cybersecurity norms is not a one-off investment, but a continuous process.
- Identify new areas for engagement and potential development of 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 states continue to exploit. It is likely that as technology evolves, even more of these will become apparent.
- Drive greater understanding of how international law applies to cyberspace. The PoA should encourage states to articulate their positions on international law and then collect them, building a common understanding of this critical area.
- Establish liaisons with regional organizations 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.
- Drive global cybersecurity capacity building, in collaboration with stakeholders across sectors, in support of the Sustainable Development Goals, to allow for state implementation international expectations in cyberspace. This could include the identification of gaps in cybersecurity capacity building efforts and help devise implementation solutions to fill those gaps.
- Identify potential avenues to limit the use of private sector offensive actors (i.e. "cyber mercenaries") 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.
- Develop sustainable models for multistakeholder diplomacy. The PoA by itself needs to be a multistakeholder initiative, but that does not mean it should to be static. In fact, the PoA should dedicate time and effort to explore existing barriers to multistakeholder inclusion and identify good practices to mitigate exclusion – at international levels and domestically.
- Finally, since 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.