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 third substantive session of the Open-Ended Working Group on security of and in the use of information and communications technologies, July 25-29, 2022

Microsoft welcome the opportunity to submit our response to the third substantive session of the Open-Ended Working Group on the security of, and in the use of, information and communications technologies (OEWG). Our submission addresses both the questions posed by the Chair in his June 22 letter and the recommended next steps outlined in the draft progress report. We hope our inputs prove useful and we remain ready to offer additional contributions. We also highlight our commitment to capacity building. However, we believe that the multistakeholder community can contribute valuable experience and expertise on *all* aspects of the OEWG mandate and have drafted our response accordingly.

Given this, it is disappointing that few states chose to politicize the accreditation process by blocking over one-third of non-governmental stakeholders – those without ECOSOC accreditation - from taking part in the OEWG deliberations. Many of these stakeholders have contributed significantly to delivering an online world that is safer, more secure and more respectful of rights; their work remains highly pertinent to the scope and purpose of the OEWG. Furthermore, we are concerned that a disproportionate number of those blocked represent industry voices – including that of Microsoft. This is a group of stakeholders uniquely positioned and equipped to help protect the online environment.

Given that the vast majority of the 32 organizations come from one UN regional group, we fear that the decision to block may have been politically motivated, rather than recognizing the relevance of the expertise and experience these organizations can bring into OEWG deliberations. For this reason, we urge states to find a sustainable way of including all relevant stakeholders in UN discussions on ICT security. Meanwhile - despite the barriers to our effective participation - we will continue to engage constructively with the OEWG wherever possible, in pursuit of our common goal of a safe and peaceful online environment for all.

Guiding questions for discussions with stakeholders at the third substantive session of the OEWG

1. What are the various ways in which stakeholders are currently involved in supporting and/or delivering capacity building initiatives in the context of the current ICT security capacity-building landscape?

Microsoft highlight the importance of technical and cooperative measures in capacity building, such as sharing technical information - including threat intelligence and compendia - and developing and disseminating comprehensive good practices. The multistakeholder community has, and can continue to, drive many of these efforts. For its part, Microsoft have contributed to various cybersecurity capacity building initiatives around the world, including:

- ***Supporting the Global Forum on Cyber Expertise:*** Microsoft have supported the Global Forum on Cyber Expertise (GFCE)[1] since its inception and remains active within its working groups. In addition,

[1] Global Forum on Cyber Expertise, https://thegfce.org/

we helped create the GFCE-Microsoft Africa program fellowship, which focuses on mapping and streamlining existing cybersecurity capacity building efforts in Africa.[2]

- ***Working to deliver sound national cybersecurity practices through the International Telecommunications Union (ITU):*** Microsoft played a key role in the ITU, helping develop a '*National Cybersecurity Strategy Guide*'[3], and we have continued to support efforts to adopt national cybersecurity strategies around the world, particularly in developing countries.
- ***Promoting good practices on critical infrastructure protection with regional organizations:*** Microsoft have worked with the Organization of American states (OAS)[4] for many years to promote good practices, particularly in critical infrastructure protection and in addressing cybercrime. Many of the initiatives we promote are built on our experience in providing technical support to organizations in critical sectors around the world. We therefore encourage the OEWG to hold dedicated interactive sessions on protecting critical infrastructure across sectors and would welcome the opportunity to share our insights.
- ***Election security and healthcare sector compendia*:** Microsoft joined efforts with the Alliance for Securing Democracy (ASD) and the Government of Canada in producing a Compendium on Countering Election Interference.[5] This provided concrete recommendations and good practices critical to electoral infrastructure and were welcomed by practitioners. Building on the success of this, we partnered with the CyberPeace Institute (CPI) and the Government of the Czech Republic to compile a compendium of cybersecurity best practices for protecting the healthcare sector from cyber harm (another critical sector highlighted by the first OEWG).
- ***Partnering with the United States Telecommunications Training Institute (USTTI):*** Microsoft have helped the USTTI deliver training to equip officials from emerging economies with the skills needed to deploy wireless technologies, implement national cybersecurity strategies, support internet deployment, launch cloud services and ensure sound emergency communications plans – all while working to support the rule of law.
- ***Helping build the resilience of non-profit organizations:*** One example is the CPI's *CyberPeace Builders* program, which works to increase the resilience of non-profit organizations around the world through a corporate network of volunteers.[6] Microsoft is a proud supporter of this initiative, contributing both staff and funding.
- ***Protecting critical democratic processes through Microsoft AccountGuard***: In 2018, we launched a not-for-profit service designed to protect organizations underpinning democracy from cyberattacks. This is available free-of-charge to eligible bodies and has three core offerings: 1) unified threat detection and notification across accounts, 2) security guidance and ongoing education, and 3) early adopter opportunities enabling us to collect critical feedback and rapidly update security to address the specific needs of qualifying organizations.[7]

[2] GFCE and Microsoft announce an investment partnership in Cybersecurity Capacity Building in Africa – Global Forum on Cyber Expertise (thegfce.org), 2020

[3] ITU, National Strategies, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

[4] OAS and Microsoft, "*Report with Recommendations to Mitigate Cyber-attacks on Critical Infrastructure in Latin America and the Caribbean*", 2018, https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-009/18

[5] Multi-Stakeholder Insights: A Compendium On Countering Election Interference – Alliance For Securing Democracy (gmfus.org), April 2021

[6] CyberPeace Institute (CPI), Cyber Builders Program, https://www.cyberpeaceinstitute.org/cyberpeacebuilders

[7] Protecting democracy with Microsoft AccountGuard - Microsoft On the Issues, 2018

- ***Microsoft's cybersecurity skilling initiative:*** In 2021, Microsoft announced a cybersecurity skills initiative in the United States, which has since expanded to embrace 23 other countries.[8][9] One of our goals is to ensure that those populations traditionally excluded have opportunities to enter the field of cybersecurity, thus helping address global skill shortages.
- ***Sharing threat information:*** Microsoft see transparency and information sharing – both with our customers in government and more broadly - as essential to protecting the digital ecosystem. We serve billions of customers globally, placing us in an ideal position to generate a unique and detailed insight into the current state of cybersecurity. For example, we recently released two reports detailing the relentless, destructive, state-sponsored cyber operations we have observed in the hybrid war against Ukraine.[10][11]

2. What capacity-building initiatives or projects can stakeholders most meaningfully and effectively contribute to? Are there certain types of initiatives (e.g., technical training, skills training) that present particularly suitable opportunities for meaningful and effective contributions from stakeholders?

The multistakeholder community is taking part in numerous capacity-building initiatives; implementing norms, driving cybersecurity hygiene, establishing national strategies, providing clarity on applying international law in cyberspace, developing incident response plans and emergency management, and protection of critical infrastructure, to name only a few. In fact, we would be hard-pressed to find examples of cyber capacity building where stakeholders did not or could not add value. There are numerous examples of successful multistakeholder projects that directly address these areas and equally numerous reasons why it is important to embrace such an approach. Noteworthy examples include:

- The cocreation of compendia on election and healthcare sector cybersecurity, which identified threats and made concrete recommendations and good practices to strengthen collective capacity. The practical type of collaboration shows the value of differing perspectives in developing guidance that others can put into practice.
- The Oxford Process on International Law Protections in Cyberspace[12] has already produced five so-called 'Oxford statements' on the applicability of international law in cyberspace, each signed by more than 100 legal experts. The statements focus on 1) International Law Protections against Cyber Operations targeting the Health Care Sector, 2) Safeguarding Vaccine Research, 3) International Law Protections against Foreign Electoral Interference through Digital Means, 4) the Regulation of Information Operations, and 5) Activities, and the Regulation of Ransomware Operations. These statements have informed and galvanized international deliberations on the applicability of international law and are frequently referenced in expert discussions, including at the UN.
- The '*Let's Talk Cyber*'[13] initiative stimulated discussions between governments, civil society, and industry, helping raise the profile of ongoing multilateral discussions at the UN, and in particular the OEWG. The support from the governments of Australia and Canada in particular added immense value to the overall effort. This is an excellent example of successful stakeholder collaboration and

[8] Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries - The Official Microsoft Blog, 2022

[9] Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Germany, India, Ireland, Israel, Italy, Japan, Korea, Mexico, New Zealand, Norway, Poland, Romania, South Africa, Sweden, Switzerland, and the United Kingdom.

[10] The hybrid war in Ukraine - Microsoft On the Issues, April 2022

[11] Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues, June 2022

[12] The Oxford Process, Oxford Institute for Ethics, Law and Armed Conflict, https://www.elac.ox.ac.uk/the-oxford-process/

[13] https://letstalkcyber.org/

provided a vehicle for meaningful multistakeholder deliberations. Moreover, it helped create a community of trusted partners that can be leveraged in the future.

These examples show the genuine benefits of multistakeholder initiatives to the OEWG. At the same time, they demonstrate that diversity among stakeholders, bringing a range of perspectives and expertise, can offer varying types of support to capacity building. While contributions from government, civil society, industry, and academia vary they will be complementary and essential for advancing shared goals. This is why we believe multistakeholder engagement in capacity building is essential across all OEWG issues.

That said, Microsoft urge the OEWG to consider the multistakeholder community – in particular, the private sector – as more than simply a potential source of funding or merely a stakeholder for capacity building. The multistakeholder community can bring invaluable experience and expertise - and not just in implementation. This requires giving them the opportunity to participate meaningfully in OEWG deliberations, particularly where new ideas or commitments are being discussed. Such participation for the multistakeholder community would also help ensure that capacity-building efforts provide more than simply one-off, ad-hoc initiatives.

3. What forms of stakeholder involvement (e.g., contribution of technical resources, co-creation of programs, contribution of time and expertise of skilled individuals) work well and what forms of stakeholder involvement work less well?

Microsoft believe in the value of multistakeholder engagement in helping establish a safer and more secure online world. This is why we have prioritized advancing shared goals with our partners in civil society, academia, and government. The earlier examples show the vital role of engagement in internet governance, which by definition is multistakeholder in nature. Therefore, the number of projects currently ongoing or the varying forms of stakeholder involvement is less important than the bringing together of different expertise and cross-sectoral experiences, united in pursuing a common goal.

Given that cyberspace is predominantly owned, operated, and maintained by the private sector, it is hard to envisage meaningful stakeholder involvement without the input and participation of those very organizations responsible for maintaining much of the fabric of the domain. Meanwhile, victims of cyber incidents are frequently private organizations that wind up with access to valuable information about how attacks were conducted and/ or mitigated. Finally, as human interactions and activities increasingly shift online, decisions taken in the interests of security have implications for human rights and free expression, requiring input from academic and civil society organizations to ensure these are adequately defended. Given this, we believe it is counterproductive to restrict the inclusion and participation of the broader multistakeholder community. These stakeholders can bring unique insights offer, collectively and individually, in both capacity building and in the wider ICT security sphere more broadly.

Guiding question on how stakeholders can contribute to the implementation of the concrete, action-oriented proposals made by states at the first and second substantive sessions of the OEWG.

1. With regard to the concrete, action-oriented proposals made by states at the first and second substantive sessions of the OEWG as captured in the draft annual progress report, are there any specific proposals which stakeholders can most meaningfully and effectively contribute to the implementation of, given their unique expertise, resources, knowledge and experiences. If so, which proposals are these, and in what way can stakeholders contribute to their implementation?

Microsoft welcome the insights in the draft progress report. Nevertheless, we urge the OEWG to recognize that stakeholders can make valuable contributions to all the proposals and recommended

steps included in the draft report. Thus they should have a systematic, sustained, and substantive role in implementing the OEWG recommendations and not restricted to specific areas such as information-sharing, critical infrastructure protection, and supply chain security, as set out in the current draft.

Microsoft encourage states to take a wider view of cybersecurity confidence-building measures (CBMs) and move beyond conversations limited to states only. Effective implementation of CBMs in this space needs to be informed by the experience and expertise of relevant stakeholders. Industry needs to be involved in any response to a significant cyberattack at both domestic and international levels – including transborder infrastructure operators delivering services across members states or globally. This makes it important that points of contact are clear on both the industry and technical community side as well as government. Similarly, CBMs might apply when it comes to building trust with the industry, potentially through putting in place processes that help governments understand the security protections being used in a particular product or service.

2. With regard to the concrete, action-oriented proposals made by states at the first and second substantive sessions of the OEWG as captured in the draft annual progress report, are there any specific proposals which can be expanded to cover stakeholder groups? To consider one example, can a parallel Points of Contact directory be created by stakeholders to cover key contact points in the private-sector and technical community?

Microsoft appreciate the Chair's decision to structure the report around concrete proposals and recommended steps. Given this focus, a parallel Points of Contact directory created by stakeholders to cover key contact points in the private sector and technical community could prove worthwhile, but only if connected to the efforts led by states.

This is true for the various proposals included in the draft report. It is important that the multistakeholder community participate in a common effort, rather than pursue separate tracks that would duplicate work on the initiatives in the draft report. Cybersecurity requires a whole-of-society approach; creating an artificial demarcation between states and industry and civil society at international level would prove counterproductive. Additional suggestions for stakeholders' role in implementing the action-oriented proposals by states are detailed below.

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

Microsoft's response to elements included in the OEWG draft progress report

Microsoft welcome the various action-oriented proposals in the draft report for the OEWG to advance in the upcoming sessions. We also recognize the challenges involved in multilateral negotiations and the Chair's intention to focus on the '*low-hanging fruit*' such as adopting CBMs at UN level.

Nevertheless, we believe that the current negative trends in cybersecurity demand a more ambitious and forward-looking response from the international community. In particular, the report could outline ways to advance international discussions on norms, to address the constantly evolving threat landscape. Concrete steps could include further guidance on existing norms and how to implement them. Another area for action is in international law, in particular in identifying gaps in the existing legal framework and developing measures to advance accountability for cyberattacks.

Existing and potential threats

Microsoft welcome references in this section on strengthening interactions between states and relevant stakeholders, including businesses, non-governmental organizations, and academia, through the exchange of knowledge and best practices on the protection of critical infrastructure and critical information infrastructure. While this area is crucial, we would also welcome the report to encourage broader collaboration between states and the stakeholder community on addressing existing and potential threats.

As it stands, the draft leaves this to bilateral and voluntary collaboration engagements between states and relevant stakeholders. Furthermore, in this section bullet 'a' and recommended step 2 limits the sharing of risk assessments and technical information - including threat intelligence and relevant compendia - to states alone. This is unfortunate, as it is the stakeholder community that is the main driver for information-sharing, threat analysis, and cutting-edge research. Conducting this cooperation solely via bilateral exchanges could be challenging for smaller states, which may lack adequate capacity or opportunity. The report could offer proposals on how the OEWG could systematically strengthen exchanges on threats with the broader multistakeholder community for the benefit of all states.

Microsoft welcome the call for specific measures to safeguard the so-called '*public core*' of the internet, i.e. its availability and integrity.[14] As this public core includes both the digital architecture and the physical transmission media, we encourage states to, at future sessions, discuss specific components of critical infrastructure essential to internet's functioning. In particular, the OEWG should recognize growing ICT threats against physical infrastructure, such as underseas cables and space assets, which perform key functions in delivering internet services regionally or globally. A recent cyberattack against KA-SAT network demonstrated that even limited cyberattacks on infrastructure can have cascading impacts internationally.[15] The OEWG should therefore discuss specific measures and good practices to increase cyber resilience of assets essential for protecting this public core. We would also urge states to adopt stronger language on ensuring the integrity of the supply chain and preventing the use of harmful hidden functions. Currently, the report simply calls for greater "*cooperation and assistance*". Ideally, the text should also call for "*concrete measures*", as is the case for other recommendations in this section.

Finally, given the OEWG's mandate to address international peace and security issues, Microsoft suggest that this may not be the most appropriate forum for advancing measures and initiatives on data security. Data security is a multifaceted issue, one that affects governments, organizations, and individuals. It requires consideration of existing national rules and international legal regimes beyond the scope of

[14] Global Commission on the Stability of Cyberspace (GCSC), Call to Protect the Public Core of the Internet: https://cyberstability.org/news/global-commission-proposes-definition-of-the-public-core-of-the-internet/

[15] KA-SAT Network cyberattack overview: www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

the First Committee and its subsidiary bodies. These include rules governing data protection, privacy, and intellectual property to name only a few. OEWG action on this could therefore have unforeseen consequences for the global economy, particularly on limiting data free flows and the use of open data for research and sustainable development. Therefore, any measures should align with existing data protection and privacy.

Rules, norms and principles of responsible state behavior

We welcome references encouraging states to make use of the online self-assessment UNIDIR 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 originally proposed by Australia, Mexico and others. This aligns with the recommendations in the 2021 OEWG and GGE reports, citing that "*states, on a voluntary basis, use the model 'National Survey of Implementation of United Nations General Assembly Resolution 70/237' to help them assess their own priorities, needs and resources*". A reasonable deadline for a first assessment could be the 4th substantive session.

Microsoft also support the call to develop additional guidance and checklists on norms implementation, along with establishing common understandings on technical ICT terms. Such checklists could recommend good practices and specific national level legislative, policy, institutional, technical and procedural measures to advance implementation of the existing norms of responsible state behavior in cyberspace. Combined with the UNIDIR survey of national implementation, this could help create targeted capacity building programs for norms implementation.

Microsoft welcome that the report recognizes that additional norms could be developed over time. In our view, further development of norms and their implementation are not mutually exclusive and should take place in parallel. This view, which has been confirmed in the UN Group of Governmental Experts on information security (UN GGE)2015 consensus report and affirmed in subsequent UN General Assembly resolutions, reflects the constantly changing nature of the digital ecosystem and need for adaptability. Given the ever-evolving threat landscape, Microsoft believe that - beyond recognizing this reality - the progress report should also outline ambitious and urgently needed steps on how to update the UN normative framework to better address current and future ICT threats. In particular, Microsoft believe that in light of recent trends, states should consider further steps to secure global ICT supply chains, protect humanitarian data, and restrict the use of so-called 'cyber mercenaries':

- ***Securing global ICT supply chains from evolving ICT threats:*** Recent experience suggests that existing norms around securing the ICT supply chain should be specified and advanced to avoid indiscriminate cyberattacks that target software and security update mechanisms. These can have far-reaching consequences for critical infrastructure operators globally and can undermine security and trust in the entire digital ecosystem. This new challenge jeopardizes public trust in technology and requires an urgent response from the international community.
- ***Protecting humanitarian organizations from cyber harm:*** Protecting humanitarian data, particularly following the cyberattack against the International Committee of the Red Cross (ICRC), which compromised the personal data of more than 515,000 highly vulnerable people, would be another positive step for the OEWG. We call on states to publicly affirm, in the OEWG report, that humanitarian organizations provide critical services to the most vulnerable in our communities and should be off limits to cyber harm.
- ***Limiting stockpiling and exploitation of vulnerabilities:*** In our view, limiting the use of cyber mercenaries should also be high on the OEWG agenda. This rapidly expanding industry of companies develops and sells tools, techniques and services that allow their clients - often governments - to break into networks, computers, phones and internet-connected devices. The stockpiling and selling of vulnerabilities for profit undermines trust and security in the online environment and gravely impacts human rights. Such practices also violate the spirit of norm '(j)' in

the 2015 GGE report, which calls on states to encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies. Left unchecked, the situation will only escalate and increase insecurity across the entire digital ecosystem. We recommend that states act swiftly to provide additional guidance on this norm (j).

Last, we welcome the proposal to use submissions of working papers to drive the OEWG's work on, *inter alia*, norms guidance, implementation, checklists, and building common understandings of ICT terminology. It is unfortunate, however, that this call is currently only addressed to 'states' and 'groups of states'. We recommend updating this to encourage a multistakeholder approach that combines their resources, expertise, and experience to drive work on norms implementation.

International law

Microsoft welcome the proposal to change from general exchanges of views on international law to more granular, thematic exchanges of *how* different bodies of international law apply in the ICT environment. We also welcome the idea of inviting experts, such as those from the ICRC, to deliver thematic briefings on different subjects of international law. We also support leveraging existing academic initiatives, such as the Oxford Process, to provide relevant expert briefings.

Including a non-exhaustive list of topics proposed by states for further discussion under international law - spanning due diligence to human rights issues - was useful and could offer future opportunities for more detailed discussions. Although the list is non-exhaustive, we recommend explicitly mentioning international humanitarian law (IHL), rather than just listing its core principles without referencing the relevant body of law. Additional thematic areas that could be explored include questions on how prohibition of the use of force applies in cyberspace, legal rules prohibiting the use of proxies for conducting malicious cyber activities, and the rules governing extraterritorial activities in cyberspace.

While deeper discussions on how existing international law applies online are important in setting expectations for responsible behavior, the OEWG should be more ambitious. It could also focus on identifying gaps in existing international law and strive to advance progress on this. The need to focus on identifying these gaps was highlighted by most states in previous OEWG deliberations and would be the next logical step. The OEWG could systematically map existing gaps and produce recommendations for addressing them. The work of the Oxford Process, on how bodies of existing international law apply to specific sectors (such as healthcare) or how established legal rules (such as due diligence) relate to ICTs, could be used as a model.

Here, we restate our previous proposal for an OEWG process to create a mechanism that would hold states accountable for publishing their views on how international law applies, albeit on an informal basis. It was positive to see concrete, action-oriented proposals on international law by states in the report, but overall, the recommended steps lack specific references to identifying gaps and exploring the need for additional legal obligations based on those gaps.

Lastly, Microsoft caution against using the term "*mutual legal assistance*" in international peace and security discussions. This term is commonly understood as implying cooperation in sharing information and evidence during criminal investigations. Specifically, the section on threats (bullet 'vi') and the proposal in the section on international law (bullet 'c') for *"improving mechanisms of mutual legal assistance for investigating malicious use of ICTs*". While we fully support this idea in principle, we believe it falls outside of the remit of the UN First Committee and its subsidiary bodies.

Confidence building measures (CBMs)

Microsoft support establishing UN CBMs as tools for reducing tension, minimizing the risk of misperception and building trust. The UN has yet to adopt cyber-specific CBMs and such a step would

be welcome. There has been significant progress on CBMs in regional organizations, including on those adopted in the Organization for Security and Cooperation in Europe (OSCE).[16] Thus we advise the OEWG not to duplicate efforts, but to learn from existing regional efforts, identify good practices, and encourage their widespread adoption. In short, to focus on aiding implementation or amplification of previously agreed CBMs.

The proposal in the progress report, for the OEWG to establish a global points of contact (PoC) directory on ICTs at the UN, is welcome. It should cover all relevant stakeholders, including private sector entities and operators of critical infrastructure globally. That said, we continue to argue that the UN need not create its own list, but instead build on successful efforts in regional fora, such as the EU or the OSCE.

Microsoft also support the idea of convening an intersessional meeting with all relevant stakeholders to develop and implement additional CBMs beyond the proposed PoC network. We support the proposed focus on supply chain, preventing malicious uses of ICTs tools and techniques and of harmful hidden functions, and sharing of current threat information. Beyond these, we also recommend examining additional CBMs that foster private-public partnerships to counter ICT threats and to establish global procedures for the coordinated disclosure of vulnerabilities among relevant stakeholders.

Finally, stronger references to the use of the UNIDIR Cyber Policy Portal as an avenue for sharing information (e.g., White Papers, national strategies and policies including ICT capabilities, information on national ICT institutions and structures, and national lists of critical infrastructure) would be welcome. We also encourage states to further fund the UNIDIR Cyber Policy Portal. In many ways, the Portal and the information it offers is a CBM in its own right. In line with our previous submission, Microsoft believe that the OEWG can be act as a 'forcing function' for states to act, implement, and publicly report on their cybersecurity norm implementation and CBM-related efforts.

Capacity building

We commend the emphasis on stepping up cybersecurity capacity building globally, including by coordinating and integrating activities within larger development programs and multi-donor trust funds. This would deliver an outcome that Microsoft have advocated for since the launch of the first OEWG, i.e., mainstreaming cybersecurity capacity-building efforts into the broader UN digital development agenda, as exemplified by the Sustainable Development Goals. In our view, the OEWG is uniquely positioned to improve the security and stability of cyberspace by promoting cybersecurity capacity building to a broader audience.

We also welcome the recommendation to establish a trusted UN focal point with responsibility of coordinating offers and requests for capacity-building assistance. When the UN focal point is established, we urge states to closely coordinate these efforts with organizations that have long-established experience and greater visibility into activities and programs in this domain, such as the GFCE. Such an approach would ensure a truly global collaboration for the benefit of all states, whilst avoiding competition and duplication of efforts.

We also strongly support the suggestion that the OEWG could help improve understanding of capacity-building needs in developing countries. This effort is needed to design tailored capacity-building programs; participation by states in the UNIDIR's survey of national implementation (discussed above) would help here. We also encourage the UN Secretariat and UNIDIR to work with the GFCE and other relevant stakeholders to analyze the results of this survey and present the outcomes at future OEWG sessions. As well as building understanding into the needs of developing countries, the OEWG and the

[16] Organization for Security and Co-operation in Europe (OSCE), Cyber/ ICT Security, https://www.osce.org/secretariat/cyber-ict-security

UN Secretariat could also assist those states currently lacking the resources to meaningfully engage in UN discussions on cyber processes.

The Chair could convene a set of meetings – open to all relevant stakeholders – focusing on building the capacities states require. As already discussed, forums such as the GFCE could play an important role; it is an initiative that the OEWG could consider working with and expanding in future. Opening this to other stakeholders would also help ensure a greater understanding in the multistakeholder community of the topics and challenges that the OEWG is addressing.

Last, it is important to remember that capacity building needs to be treated as a continuous process - one with short- and long-term objectives - rather than one-off engagements. Therefore, we are encouraged to see a reference to states considering the establishment of a permanent mechanism for exchanging views and ideas related to capacity building in ICTs in the draft progress report. Here, we stress the importance of establishing a permanent UN body responsible for this thematic area. We elaborate further on this below.

Regular institutional dialogue

Microsoft have closely followed, and whenever feasible provided input to, various UN initiatives and dialogues on cybersecurity over the past two decades. This has included, *inter alia*, the multiple iterations of the UN GGEs as well as the current and previous OEWGs.

Unfortunately, as we have repeatedly stated, the overall security of the online environment continues to deteriorate. This is despite the progress in building an international framework for peace and stability in cyberspace that has resulted from these dialogues. The number of countries investing in offensive cyber capabilities continues to increase, and attacks have grown more frequent and more sophisticated, in seeming disregard of international expectations. The situation is made worse by the current, unlawful invasion of Ukraine.

Given this, there must be greater efforts at international level to increase the security and stability of cyberspace. There needs to be a regular and ongoing dialogue between all interested parties on these critical issues. Microsoft believe that it is time to establish a permanent UN forum broadly focused on cybersecurity issues – one that allows meaningful multistakeholder participation.

We welcome the fact that many states support creating a permanent body under the auspices of the UN that would include support for norm implementation and capacity building. The proposal for a *Programme of Action* (PoA)[17] was positively referenced, something Microsoft strongly support. Related references in the report are therefore welcome. However, we hope that the PoA is adopted as soon as possible and that it focuses on more than simply capacity building. We believe that the PoA should be a permanent, standalone body, rather than tied to the OEWG with a time-limited mandate. Moreover, it needs to be able to navigate in an area that values speed and innovation, meaning that it should retain sufficient flexibility for states to agree on future new areas of work.

There is little doubt that such a PoA would be a positive contribution to UN cybersecurity processes. Its establishment would send a strong signal of commitment by states to preventing, combating, and eradicating threats emanating from cyberspace. Moreover, it is envisioned to serve as a permanent, more structured yet flexible solution that allows for consensus driven, action-oriented and transparent regular dialogue between states, more multistakeholder engagement, and acknowledges the importance of capacity building. Such a structure would ensure both sustainable funding and incorporate existing processes into a single, permanent, mechanism, avoiding the need for a regular renewal of mandates and the associated political risk that comes with it.

[17] United Nations, The future of discussions on ICTs and cyberspace at the UN, 2020, joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf (un-arm.org)