Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

September 13, 2018

Microsoft submission to the Background Paper to the IGF Best Practice Forum on Cybersecurity

Microsoft appreciates the opportunity to review and comment on the *Background Paper on Cybersecurity values, culture and norms* developed by IGF's Best Practice Forum on Cybersecurity. We hope that our submission underscores our appreciation of the important work of the Internet Governance Forum (IGF) and its Best Practices Forum (BPF) working group on cybersecurity and norms development. Ensuring a diversity of perspectives in this dialogue, representing different nations, sectors, and citizens across the digital divide, is essential for the online environment to continue to thrive.

In the first part of our response, we seek to provide comments and nuance on the actual background paper itself, which we hope will help improve the final output of the group. Following that, we provide responses to the questions that were highlighted in the request for input; whilst interpreting some of them in line with more established concepts and terms.

General feedback on Background Paper

Overall, Microsoft feels aligned with the draft Background Paper released by the BPF, and feels it approaches the subject of cyber norms development with an appropriately holistic perspective, recognizing the importance of a "cybersecurity culture" and highlighting the potential impact of norms development across the digital divide. In addition, we applaud the decision to recognize cybersecurity as a dynamic and shared responsibility, as states, industry, civil society and even individuals all have critical roles to play in promoting greater cybersecurity.

However, while we are enthusiastic about the paper being developed, the following are meaningful ways we feel it could be improved:

- Perhaps most importantly, the paper on several occasions seems to conflate "norms" with "law," and while norms may evolve into law – as the paper describes early on – they are not themselves legal frameworks and the distinction should be made clear throughout.
- While the paper recognizes the importance of multistakeholder engagement in norms development, it could do more to emphasize that civil society has an important role to play in holding states and private industry accountable to emerging norms. Particularly in cyber norms development, this type of engagement we feel has been too often absent and is worth remarking on.
- In describing the process of early-stage norms development, the paper introduces the concept of "authoritative bodies" which traditionally establish norms, without further explanation of what constitutes an "authoritative body." Especially in the cyber norms context, this would be helpful to explain further.
- When the paper discusses the NIST framework, it neglects to mention that it has started to evolve into an ISO standard – indicating that it is being accepted at an international level as a norm.
- In the paper, "unilateral action" should be highlighted as one way of signaling the recognition and acceptance of new norms. Once norms have been established, it is important to see unilateral action on the part of industry, civil society and governments insisting that the norms are adhered to.
- Finally, Microsoft recently joined with other global technology companies in signing the Cybersecurity Tech Accord – a statement of principles on cybersecurity and an ongoing effort by industry to improve cybersecurity for users and customers everywhere. Given the scale of the initiative, its potential impact, and its relation to the subject of the paper, we feel its recognition would be a worthy inclusion about innovative efforts by non-governmental stakeholders to advance norms and collaborate on international cybersecurity solutions.

Responses to questions

1. *How do you define a culture of cybersecurity?*

The importance of developing and maintaining a culture of cybersecurity cannot be overstated as the world pursues the benefits of digital transformation – at national, organizational, and even individual levels. From an organizational perspective, Microsoft is committed to building an intentional internal culture that prioritizes the cybersecurity of our products and customers. This commitment manifests itself in a myriad number of actions, large and small, including regular employee trainings, internal cybersecurity audits, and a "secure by design" process that includes a Secure Development Lifecycle (SDL) and Operational Security Assurance (OSA) framework for our products.

In addition, Microsoft believes that as a leading technology company and a first responder in cyberspace, we have a responsibility to empower others in society to make responsible cybersecurity choices. Microsoft has long played a role in socializing and promoting cybersecurity awareness in the public and private sectors, and has worked to support the development of informed and effective cybersecurity policies. To this end, we have published universally-available policy guidance, including recently published papers on security baselines for critical infrastructure protection and national cybersecurity policy frameworks.

2. *What are typical values and norms that are important to you or your constituents?*

Microsoft believes that the technology sector has an important role to play in promoting a healthy cybersecurity culture, and has spearheaded such efforts through its engagement with the Cybersecurity Tech Accord, a group of over 40 global technology companies committed to 4 foundational cybersecurity principles:

i. We will protect all of our customers and users everywhere

ii. We will oppose cyberattacks on innocent citizens and enterprises

iii. We will help empower users, customers and developers to strengthen cybersecurity protection

iv. We will partner with each other and with likeminded groups to enhance cybersecurity

The Tech Accord is the first-ever global coalition of industry partners, of its size, to come together over foundational cybersecurity principles and commitments. Having such a stated set of industry principles and values has never been more important, as the scale of threats online continues to escalate. Amidst increasingly sophisticated criminal activities and aggressive state behavior online, it was important to be clear to our customers everywhere – those who rely on our technologies – where we stand and how we can help.

3. *Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.*

In 2017, Microsoft President Brad Smith issued a call for a Digital Geneva Convention, a proposed legally-binding agreement between nations about sensible limitations on state-sponsored cyberattacks against civilians and critical infrastructure in times of peace. While a formal convention is likely years away, there has been important progress made by state and civil society organizations to establish and recognize international norms for cyberspace. This includes the norms development work done by the Global Commission on the Stability of Cyberspace (GCSC), as well as the norms agreements and norms-related agreements reached by states at the UNGGE, G20, G7, SCO, OSCE and in other forums, which we are glad to see described in detail in the BPF paper.

4. *Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?*

As referenced above, norms may evolve into law, depending *inter alia* on the political will of the relevant decision-makers and stakeholders as a whole. Indeed, a discussion of norms – i.e. how the status quo *should* be, or what the relevant stakeholders *should* or *should not* be permitted to do – likely preceded the adoption of most conventions and legally-binding agreements in general.

In fact, such a discussion, elaboration and, ideally, adoption of norms can reasonably be described as a *prerequisite* for the establishment of binding legal agreements. It is in this push towards an ongoing discussion on how the status quo *should* be, that norms are most beneficial. They are essential in facilitating an ongoing discussion and dialogue among stakeholders who may not (yet) be ready to discuss binding legal agreements.

5. *Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?*

Despite the development of new norms for cyberspace in various forums representing different stakeholder groups and state organizations, no single set of international cybersecurity norms have been recognized or adhered to by nation states. In the absence of recognized norms, the escalating instability of cyberspace continues unabated. Perhaps the most recent examples of this escalating behavior are the Russian cyberattacks against political and civil society institutions within the US in August 2018.

What is needed now is the consolidation, interpretation, and universal recognition of the norms that have already been agreed to at the regional and multilateral level by governments around the world. This consolidation would effectively set the baseline for future and ongoing discussion on, and negotiations of, the issue. With a salient list of internationally-recognized cybersecurity norms, endorsed by a multistakeholder coalition including national governments, the international discourse could then turn to the promotion of the norms and to accountability efforts.

6. *What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?*

For the voluntary norms that have been developed for cyberspace to meaningfully curb irresponsible state behavior, they must be more widely recognized, respected and insisted upon by nations, industry and civil society alike. When norms are violated, such violations must be clearly identified and denounced by all who were impacted. Attacks such as NotPetya, which so significantly damaged companies including Maersk and FedEx, should not be accepted as the new normal but rather denounced as violations of international norms in cyberspace. Such denouncements must be prolific and continuous, and demand an improvement of the status quo.

This challenge of reinforcing cyber norms is exasperated by the difficulties associated with accountability following cyberattacks. In the wake of cyber incidents today, perpetrators are rarely ever accused of malfeasance, and never truly held accountable for their actions. When attribution does occur, it is done by individual states or small coalitions of like-minded nations and based on investigations that are never made public. Unsurprisingly, this process results in denials and is without any meaningful accountability. What is needed is an independent, multistakeholder body – with international credibility – to conduct impartial forensics following cyberattacks and to provide evidence to the international community free of any semblance of bias.

7. *Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?*

More than "better" or "worse" cybersecurity, the digital divide between nations results in different challenges for countries based on their respective states of digital transformation as well as their unique sociopolitical and geopolitical contexts. Nations whose citizens and businesses are coming online today are entering a sophisticated cybersecurity environment both in terms of threats and opportunities. While they face a steep learning curve in navigating dangers online, they also have the potential to leverage new technologies to leapfrog the challenges that plagued previous generations of internet users.

Countries coming online today can benefit from applying international best practices, such as the Budapest Convention on Cybercrime, and the NIST framework, to avoid unnecessary pitfalls. These are tools that have been proven through iterative development to improve national cybersecurity. Unfortunately, nations too often still start from scratch when it comes to cyber policy – a process that can take years during which they could otherwise be working on further improving their national cybersecurity posture and culture.

To conclude, we would like to once again thank you for the opportunity to provide comments on your initial paper on the critical topic of cybersecurity culture, value and norms. We look forward to our continued discussion through the Best Practice Forum and at IGF and welcome additional opportunities to work with you on this important initiative. Should you have any questions that emerge on the basis of our responses, please do not hesitate to contact me directly, or to reach out to a member of my team.

Yours sincerely,

Angela McKay

Senior Director, Global Security Strategy and Diplomacy

Microsoft Corporation