Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

September 20, 2019

Microsoft contribution to the 2019 IGF Best Practice Forum on Cybersecurity

Microsoft would like to thank the Internet Governance Forum's Best Practice Forum on Cybersecurity (BPF) for undertaking its important work with an inclusive, multistakeholder approach, and for welcoming further input from all stakeholder groups in this study on the advancement and implementation of international norms in cyberspace. Microsoft is a strong proponent of greater multistakeholder diplomacy to promote a safer and more secure online world, and we are glad to respond to this call for contribution.

See below for our responses to the questionnaire released by the BPF, and please let us know if any further clarification is necessary by reaching out to Kaja Ciglic on Microsoft's Digital Diplomacy Team (kaja.ciglic@microsoft.com).

1. **Is your organization a signatory to any of the agreements covered, or any other ones which intend to improve cybersecurity and which our group should look at? If not, we are still interested in your opinion on the rest of this questionnaire!**

   From the list of agreements in this study, Microsoft has signed, endorsed, or supported the following:

   - *The Cybersecurity Tech Accord* – Microsoft was one of the founding 34 company signatories;
   - *The Paris Call for Trust and Security in Cyberspace ("Paris Call")* – Microsoft endorsed this agreement both as an individual company and as a signatory to the Cybersecurity Tech Accord;
   - *Mutually Agreed Norms for Routing Security (MANRS)* – Microsoft has endorsed this initiative;
   - *Global Commission on Cyber Stability (GCSC) Singapore Norms Package* – Microsoft has been a supporter of the Commission's work.

2. **What projects and programs have you implemented or have seen implemented to support the goals of any agreements you signed up to? Do you have any plans to implement specific projects?**

   Microsoft's priority when it comes to supporting agreements on cybersecurity – regardless of whether they are multi-stakeholder or industry-specific – is always to help further improve security for our users and customers. This means supporting agreements that highlight or promote best practices for technology security to improve our products and services. This also means supporting agreements that promote greater security for the entire ecosystem of the public internet, with important roles to be played by industry, civil society, and governments alike.

   Microsoft is deeply committed to the security of its products and services, spending over $1 billion dollars each year on security alone and with thousands of employees in security-focused roles. As a result, there are certainly more security programs across our different product groups than there is space to share here, each of which are intended to express the spirit of our commitments reflected in the different agreements we support. So instead of an exhaustive accounting, what follows are

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

descriptions of just a few Microsoft initiatives and programs that reflect key elements of agreements we have recently supported in order to i) improve the security of our products and services, ii) strengthen the broader cybersecurity ecosystem, and iii) encourage responsible behavior by governments to limit cyberattacks and the proliferation of cyberweapons. Associated agreements and their corresponding principles are included in italics following each description.

I) Improve the security of Microsoft products and services

- Microsoft utilizes and has published its coordinated vulnerability disclosure policy, which ensures that any known vulnerabilities in our products are reported and remediated in a timely and systematic fashion that puts customer security first. This is also in keeping with a recently-announced Cybersecurity Tech Accord commitment to have all company signatories adopt vulnerability disclosure policies by the end of the year.

  (Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)

- Microsoft uses its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs to improve the security and resiliency of our products and services. SDL is focused on building trustworthy software by focusing on secure design, threat modeling, secure coding, security testing, and privacy best practices. OSA minimizes risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are being followed effectively. This helps make Microsoft cloud-based services' infrastructure more resilient to attack and decreases the amount of time needed to detect, contain, and respond to threats.

  (Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)

- In developing our products and services, Microsoft is dedicated to promoting user awareness and customer control of their security environment with the most advanced tools. This includes many innovative initiatives, including the promotion of password-less security options and distributed digital identity.

  (Cybersecurity Tech Accord principle 3, Paris Call principle 7)

- Microsoft also brings together its technical, forensic and legal capabilities to work collaboratively with law enforcement around the world to combat cybercrime through its Digital Crimes Unit.

  (Cybersecurity Tech Accord principle 1, Paris Call principles 1 and 5)

- Microsoft leverages its position operating and maintaining one of the largest cloud environments in the world to scale its security responses and capabilities to protect users everywhere. This has included blocking over 5 billion malicious and suspicious phishing mails in 2018 alone, analyzing over 6.5 trillion signals each day, and investing over a billion dollars each year in security.

  (Cybersecurity Tech Accord principle 1, Paris Call principle 1)

II) Strengthen the broader cybersecurity ecosystem

- Microsoft has hosted webinars on cloud security and an upcoming webinar on IoT security as part of the Cybersecurity Tech Accord's series of webinars that is now a growing library of free resources meant to improve the cybersecurity capacities of governments and organizations around the world.

  (Cybersecurity Tech Accord principle 3, Paris Call principles 1 and 7)

- Microsoft's cybersecurity policy team regularly partners with the United States Telecommunications Training Institute (USTTI) to provide guidance and support to policymakers from across the world looking to establish informed policies on cloud security and other topics.

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

(Cybersecurity Tech Accord principle 3, Paris Call principle 7)

- As part of the Cybersecurity Tech Accord, Microsoft joins a monthly meeting of company signatories to address progress and identify new initiatives aligned with the four principles of the agreement. Work products that Microsoft has contributed to have included blogs, whitepapers, policy guidance, workshops and industry consultations on cybersecurity. The collective work products of the organization are available for review on the Cybersecurity Tech Accord website.

  (Cybersecurity Tech Accord principle 4, Paris Call principle 1)

- Microsoft has established the Defending Democracy Program to focus on protecting elections and democratic institutions and processes. This program has developed several new initiatives over the past year:
  - Amplified threat monitoring for campaigns and democratic institutions through AccountGuard, a free resource for qualifying customers, along with awareness-raising and training workshops for practitioners in this space;
  - Security optimization for campaigns using Microsoft software via M365 for Campaigns;
  - An open source software development kit (SDK), leveraging homomorphic cryptography to secure voting systems via ElectionGuard; and
  - Instantaneous verification of news sources to combat disinformation online via a partnership in launching the NewsGuard app.

  (Paris Call principle 3)

- Microsoft contributes to the development of national and international standards by leveraging our own best practices and participating in collaborative working groups and initiatives. For example, we have shared our experiences using SDL (see above) through SAFECode and as a part of an international standard for secure software development (ISO 27034). We also participate in working groups hosted by the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) to develop approaches and best practices for addressing a range of emerging cybersecurity challenges, including IoT device security and post-quantum cryptography.

  (Cybersecurity Tech Accord principle 4, Paris Call principles 1, 2, 6, 7)

III) Encourage responsible behavior by governments

- Through the Cybersecurity Tech Accord, Microsoft has joined with others in industry in encouraging policies that promote greater stability in cyberspace and discouraging those that promote instability. This has included advocacy on the importance of vulnerabilities equities processes for governments, discouraging policies that would undermine encryption, and supporting an open letter to the G7 on not undermining the security of technology products.

  (Cybersecurity Tech Accord principle 2, Paris Call principle 1)

- Microsoft has contributed as an active partner to the work of deliberative bodies that are seeking to draw attention to the dangers of escalating cyber conflict and limit irresponsible actions by governments in cyberspace. This has included contributing to the deliberations of the UN High Level Panel on Digital Cooperation which recently released its final report, and A Contract for the Web which recently released its first draft of commitments for comment.

  (Cybersecurity Tech Accord principle 2, Paris Call principle 1 and 9, GCSC norm 7)

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

- In 2017, Microsoft President Brad Smith issued a call for the establishment of a Digital Geneva Convention, a binding commitment to protect civilians from nation-state cyberattacks in peacetime.

  (Cybersecurity Tech Accord principle 2, Paris Call principles 1, 2, 5, 9, GCSC norm 7)

As mentioned previously, these are just some examples of the work Microsoft is doing to improve cybersecurity for its customers and the broader ecosystem. For more information on Microsoft's security solutions and initiatives, we encourage you to visit our website: https://www.microsoft.com/en-us/security

Similarly, the Cybersecurity Tech Accord is an active organization pursuing initiatives to improve security in line with its principles. For more information on the work of the Cybersecurity Tech Accord, we encourage you to visit their website: https://cybertechaccord.org/

3. **During our review, we identified a few key elements that were part of multiple agreements and seem to have more widespread support and/or implementation. Do you have views around the relative importance of these (e.g. by providing a ranked list), or are there any others that you consider to be significant commitments in these types of agreements?**

   Overlapping elements identified: ***Furthers multi-stakeholderism; Vulnerability equities processes; Responsible disclosure; Reference to International Law; Definition of Cyber threats; Definition of Cyber-attacks; Reference to Capacity Building; Specified CBM's; Reference to Human Rights; References to content restrictions.***

While we applaud the work the BPF is doing this year to map the various cybersecurity agreements across the globe between and among stakeholder groups, and identify overlapping elements, there are important differences between the agreements featured in this study that have implications for what elements should be prioritized in each case. For example, it may be wise to include language supporting publicly reviewable vulnerabilities equities processes in an agreement between governments, but it would make less sense in the context of an industry-based agreement like the Cybersecurity Tech Accord. It is therefore difficult to provide a "ranking" of these respective elements without further context, but nearly all are valuable components that should be included in agreements between one or more stakeholder groups. The only two we feel warrant further discussion here are "furthers multistakeholderism" and "references to content restrictions" – albeit for different reasons.

Microsoft believes that support for a multistakeholder approach to setting norms and rules for cyberspace is paramount for meaningful progress on global cybersecurity, and ought to be reflected in any cybersecurity agreement. Cyberspace is an inherently shared space, with much of it owned and operated by nongovernmental entities, largely private industry. This means successful agreements in this space will have to make room for voices from all stakeholder groups to provide input. This is what makes agreements like the Paris Call so important, opening the door to wider inclusion and cooperation in addressing these challenges.

However, while nearly all of the overlapping elements identified here may be valuable to include in certain agreements, a successful cybersecurity agreement does not require "references to content restrictions." While discussions about what content should, and should not, be tolerated online is an important national and international dialogue, it is meaningfully different than discussions of cybersecurity, and conflating them can often limit progress. Cybersecurity agreements should be focused on preventing the corruption and exploitation of technology products, limiting the proliferation of cyberweapons, and improving cybersecurity capacities, as opposed to focusing on the abuse of online platforms for hate speech, extremism or other content-based concerns.

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

4. What has the outcome been of these agreements? Do you see value in these agreements either as a participant, or as an outsider who has observed them?

At Microsoft, we see tremendous value in multistakeholder diplomacy to develop and reinforce expectations for responsible behavior online – so called, "cyber norms" – as reflected in many of the agreements featured in this study, including those we are party to. While private industry competes in the marketplace, and nations may have political tensions and rivalries, we all should be invested in a safe and secure online world that we all share. The inclusion of all stakeholder groups in the creation of these agreements reinforces the shared nature of this challenge, and the responsibilities we all have to be good stewards of the public internet and our collective cyberspace. By that same token, we feel that agreements which exclude this essential multistakeholder input often result in outcomes that can be counterproductive, either in design or implementation.

Allowing for multistakeholder participation in these agreements also facilitates the development of new relationships and partnerships. Since signing onto the Paris Call and the Cybersecurity Tech Accord, Microsoft has been contacted by governments, as well as industry and civil society organizations, to partner on related initiatives or collaborate on implementing the agreements themselves. Participation in this very call for contributions from the BPF is a testament to the foundation that has been laid for further cooperation. In this way, these agreements operate as confidence building measures in and of themselves.

5. Have you seen any specific challenges when it comes to implementing the agreements?

Many of the agreements included in this review have been invaluable in outlining the norms and rules that should guide responsible behavior online. It has also been helpful for them to be less prescriptive when it comes to how respective organizations should go about implementing various provisions. Efforts to protect critical infrastructure, strengthen cyber hygiene, responsibly handle vulnerabilities or implement the many other principles included in these agreements will likely look very different in the context of a large technology company like Microsoft as compared to a financial services firm, a civil society organization, or any number of other multistakeholder entities. Having flexibility in the implementation of agreements is a strength, as it lets each entity pursue approaches that make the most sense in their respective context.

However, while there is clear benefit in allowing for differentiated approaches in adhering to these agreements, such flexibility can also result in organizations not understanding how best to implement the provisions of agreements they have joined – or are subject to in the case of legislative actions like the NIS Directive or the EU Cybersecurity Act. This is why efforts like this call for contributions are so important, giving organizations the opportunity to share how they are approaching these commitments and their implementation and allowing for others to learn from peers and identify good practices they too would like to adopt.

Finally, it should be noted that there is a particular need for greater accountability when it comes to norms for responsible behavior by government actors in cyberspace – as identified in the UNGGE consensus reports and the Paris Call, among other agreements included in this study. Despite the clear call for, and enumeration of, responsible behavior online, we still see escalating cyberconflict threatening to undermine the integrity of our shared cyberspace. This underscores the importance now in pivoting in these international discussions to focus on strengthening the recognition of these norms and to pursue ways to make them more binding for governments to avoid unnecessary harm to civilians and the further proliferation of cyberweapons. There is no excuse for ignorance on the part of governments about what the norms and expectations are for responsible behavior in cyberspace.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

6. **Have you observed adverse effects, or tensions from any of the elements of these agreements, where specifics may be at odds with intended end results? For instance a commitment that may seem like it improves cybersecurity at first sight or tries to fix one issue, but has effects that lead to a reduction in cybersecurity?**

As mentioned earlier, we believe agreements can risk becoming counterproductive to furthering cybersecurity when they limit multistakeholder input or become overly prescriptive in their requirements for implementation. This is particularly true for the binding legislative agreements included in this study, including the NIS Directive and the EU Cybersecurity Act. Given the diversity of entities that are responsible for implementing the provisions of these legislative initiatives, a one-size-fits-all approach is rarely advisable and often undermines opportunities for innovation to further improve security from the technology sector in particular. As an example, legislation aimed at robust access management security could be well intentioned in mandating sufficiently complex passwords in certain contexts. However, that would limit opportunities for adopting many cutting-edge multi-factor authentication options which offer improved security by doing away with passwords altogether. As a rule, when establishing new legislative requirements, cybersecurity outcomes should be prioritized over respective approaches for achieving them to allow for the right balance of security and innovation.

Thank you once again for providing Microsoft the opportunity to contribute to this year's BPF. We look forward to reading the final report and stand ready to support further action as needed to promote a more safe and secure online world for all.

Sincerely,

Microsoft's Digital Diplomacy Team