Microsoft's Contribution to Cybersecurity Best Practice Forum, August 2017

1. **How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

   Information and communication technology (ICT) is firmly established as a pillar of modern life. Constant and rapid innovation has resulted in a profound digital transformation of established social, economic and government frameworks. This transformation has brought numerous benefits, from increased effectiveness and productivity to easier access to information and learning, many of them directly contributing to the achievement of Sustainable Development Goals (SDGs).

   However, the ubiquitous connectivity has also exposed an increasing number of individuals, business and governments to new threats. Good cybersecurity practices – those implemented by vendors developing products with security in mind, those embraced by individual consumers and organizations when using technology, and those established by governments to regulate their online environment - can help manage these threats and ensure that the benefits can be retained by everyone. It is therefore critical that cybersecurity becomes a much more prominent aspect of international development, which has so far largely focused on ensuring ICT access. Policies encouraging access and cybersecurity need to be treated as two sides of the same coin.

2. **How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

   Poor cybersecurity threatens the growth of ICT both directly and indirectly. First, the Internet is a network and our ability to resist cyberattacks is therefore only as strong as its weakest link. As a result, poor cybersecurity inevitably exposes other organizations and individuals to a particular threat. Moreover, infected machines can then be used as attack vectors, which potentially can – due to their strength in numbers – overcome even the best defenses organizations have in place.

   Secondly, the perception of poor cybersecurity can lead to a diminished adoption of the newest technologies. Whilst organizations and individuals must be cyber-aware online - in line with the need for a shared commitment to cybersecurity referenced above - that should not stop them from embracing technologies that could improve their productivity or livelihood. They should be guided in their decision-making by their assessment of their individual risk and they should prioritize and manage it accordingly thereafter.

3. **Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:**

   Microsoft would recommend grouping the threats identified to avoid duplication and to help develop effective solutions and approaches. For example, DoS attacks or unauthorized access are issues related to online crime (methods of attack below). On the other hand, issues related to security of DNS or mobile devices are related to secure development of software or hardware. Furthermore, grouping similar issues together and assigning the relevant SDGs would also help with the clarity of recommendations. With that in mind, we hope the following issues would be considered in addition to, or as a way of reorganizing / grouping, the ones highlighted in the consultation document:

   - Methods of attack: unauthorized access, DoS attacks, breaches of confidentiality and integrity of information. We would recommend limiting them to breach of availability, confidentiality, integrity and privacy, rather than developing a list of possible methods (e.g. DoS attack, ransomware, phishing, etc.), as this is likely to evolve over time.

     Possible policy solutions include aligning legislative initiatives aimed to tackling cybercrime internationally (e.g. to the Budapest Convention on Cybercrime) to ensure that persecution of cybercriminals across borders is as easy as possible.

     We are of the opinion that these apply across the SDG goals, as we consider online connectivity to be essential to achieving them.

   - Security of critical infrastructures: The consultation document touches upon security of critical infrastructures on a number of occasions, including relating to security of industrial control systems, and the underlying infrastructure of the internet. We recommend that the topics are tackled collectively under the term critical infrastructures.

Possible policy solutions include developing of national laws with the aim of protecting critical (information) infrastructures and adoption of best practices in this space. In relation to that we want to highlight the work around security baselines for critical infrastructure, in particular the Cybersecurity Framework developed by the US National Standards and Technology Institute. The Framework is currently being adapted into the process of the International Standardization Organization.

This challenge applies to SDG3 (Good health), SDG7 (Affordable and clean Energy) and SDG6 (Clean Water).

- Online abuse and gender based violence: Online services have given rise to new risks and new potential for harm, especially for vulnerable populations such as children, women and the elderly. In addition, it has opened the gate for online abuse and harassment.

  Possible policy solutions include developing laws to deter online exploitation and harassment, and not inadvertently victimize the people they seek to protect. In order to raise awareness of online risks and rewards, governments should also work closely with child advocacy and victim support organizations, law enforcement agencies, industry, youth and families, as well as focus on developing public-private partnerships.

  This challenge applies in particular to SDG5 (Gender equality).

- Lack of a secure development process/ Retaining established security best practices in new technologies: Microsoft disagrees with the statement that there is no secure development process available. Over the years we have developed our own secure development processes (Security Development Lifecycle) and others have become international standards. What is a challenge is ensuring that these best practices are disseminated and included in emerging technologies, such as the Internet of Things.

  Policy solutions include ensuring that governments disseminate best practices and guidelines, raise public awareness, act as a convening force for discussions in this space, and seek to harmonize national standards in this area.

  This challenge applies to SDG8 (Decent Work and Economic Growth) and SDG9 (Industry, Innovation and Infrastructure).

- Government surveillance and freedom of expression: Essential to personal dignity and the development of human potential, freedom of expression and from government surveillance is an internationally recognized human right that must be protected by the rule of law. However, we recommend that this point is omitted from the cybersecurity best practice and is retained as a separate item of work. In our view, the focus of the group should be on the more technical challenges of protecting assets from attacks online to ensure more immediate effectiveness and clarity of purpose. We propose a similar approach to the point raised related to repurposing of information, which in our opinion should be dealt under a group dedicated to data protection.

  Nevertheless, should the decision be taken to retain it, we are of opinion that this challenge applies across the SDG goals, not just SDG2 (Zero hunger), as indicated in the document.

- (new) Lack of cybersecurity awareness: While investment in developing more secure technologies is important, ultimately cybersecurity is down to the individual. It is therefore critical that all citizens are aware and act in accordance with basic cybersecurity best practices. This is currently not the case and is particularly challenging in communities which are only coming online.

  Possible policy solutions include promotion of cybersecurity awareness initiatives (e.g. national cybersecurity month), inclusion of cybersecurity education in schools and education in general, as well as dissemination of cybersecurity best practices aimed at small and medium sized enterprises (e.g. UK government's cybersecurity essentials). In particular, we recommend greater investment and linkages are developed between development communities focusing on broadening internet access and cybersecurity capacity building groups.

We are of the opinion that these apply across the SDG goals, but it is particularly relevant to SDG1(No poverty), as it is closely related to providing online access.

- (new) Cyber resilience of cities: We know that our world is becoming increasingly urban – by 2050 the population in urban centers is expected to grow by 66 percent – and by 2025 most of the world's data will move through or be stored in the cloud at some point. And because anyone is susceptible to cyberattacks, city planning for cyber resilience is crucial.

  Possible policy solutions include developing overarching cybersecurity and cyber resilience strategies at the city level, which allow them to identify key threats, classify and prioritize critical services, set cyber resilience goals and objectives and determine the resources needed and define roles and responsibilities.

  This challenge applies to SDG11 (Sustainable Cities and Communities).

- (new) Number of women in cybersecurity: The percentage of women across STEM (science, technology, engineering and mathematics) remains low; however, the situation is even worse in cybersecurity, where women make up only 11% of the workforce. This comes at a time when we are facing a significant gap in the cybersecurity workforce, irrespective of the level of maturity of the country in question.

  Possible policy solutions include investment in early education on cybersecurity, public-private partnerships to identify opportunities for mentoring, and developing alternative paths to cybersecurity careers (not dependent on a degree in information security).

  This challenge applies in particular to SDG5 (Gender equality)

4. **Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity. This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely, we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?**

   The complexity is the reason why it is critical that cybersecurity is treated as a multi-stakeholder effort. It requires the private sector to invest in development of technology designed with cybersecurity in mind and to appreciate that security can be a benefit in the competitive landscape and not just a cost. Furthermore, the private sector must be willing to share best practices they have learnt and ensure that the general public and the governments understand how they can best apply new technologies to increase security.

   Non-governmental organizations, on the other hand, have a critical role to play in rising awareness of security best practices, and to partner with other stakeholders in promoting responsible behavior and safety online. Furthermore, they are critical in helping to ensure that other parties are held accountable for how they balance privacy and security, and other related concerns.

   Finally, governments play an essential role in protecting critical infrastructures, through for example the development of security baselines, as well as acting as a convening forum and disseminating emerging cybersecurity best practices. Furthermore, they have a core role to play in persecuting cybercriminals, as well as in developing and enforcing rules of behavior – including for states themselves – in cyberspace.

5. **What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?**

   For nearly two decades, the cybersecurity community has consistently warned of the increasing number and sophistication of cyberattacks. But now, cyberspace is being operationalized by some states as a domain for conflict, dramatically escalating the threat. In this shared and tightly integrated domain, any escalation of hostilities could result in unintended - and even catastrophic - consequences.

In light of the existing offensive cyber capabilities of some states and of the stated intent of other nations regarding future capabilities, and to define acceptable actions in cyberspace, Microsoft strongly supports the development of cybersecurity norms and has put forward a number of proposals related to them, most recently in our call for a Digital Geneva Convention[1].

Cybersecurity norms should be designed not only to increase the security of cyberspace but also to preserve the utility of a globally connected society. As such, norms should define acceptable and unacceptable state behaviors, with the aim of reducing risks, fostering greater predictability, and limiting the potential for the most problematic impacts, in particular impacts which could result from government activity below the threshold of war.

As the United Nation process on this topic seemed to have stalled, we believe progress and discussions on this topic are more critical than ever. We propose that the Best Practice Forum examines our proposal, but also those stemming from the UNGGE discussion, and that it continues the debate, discussion and promotes the broad acceptance of cybersecurity norms.

[1] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/