The Cybersecurity Tech Accord response to IGF's request for input on its ongoing work on 'Cybersecurity Culture, Norms and Value'

The Cybersecurity Tech Accord signatories welcome the work of the Internet Governance Forum (IGF), and its Best Practices Forum (BPF) working group on 'Cybersecurity Culture, Norms and Values'. The signatories are strongly aligned with the IGF's objective of promoting multi-stakeholder engagement on issues essential to maintaining a free, open and secure internet.

We believe that diverse perspectives – from governments to civil society and the private sector – must be included in this dialogue, so that we can work towards decisions that reflect and impact a wide range of vested interests. This type of multi-stakeholder coalition is, in the end, essential to the survival of the cyberspace that we all share and we are delighted to see the IGF complementing other important initiatives in this area.

To this end, the Cybersecurity Tech Accord and its signatories are pleased to submit written contributions to the 2018 IGF BPF on Cybersecurity. The main points of our response can be summarized as follows:

- We fully agree with the IGF that cybersecurity is a shared responsibility and applaud the inclusion of the section dedicated to building a culture of cybersecurity in the background paper.
- We applaud the IGF for having conducted a very comprehensive mapping of the most widely recognized norms listed in the background paper. In our view, we would encourage the BPF to work towards collective efforts that will consolidate and help universally recognize norms that have already been agreed to at the regional and multilateral level by governments across the world, rather than work on developing/identifying new norms. This would be a more effective way to help the global discourse turn to the promotion of these exiting norms and support accountability efforts.
- The impact of cybersecurity norms depends on whether they are implemented faithfully and whether offenders are held accountable. We believe that the IGF can positively contribute to important multi-stakeholder discussions on how we can ensure effective and impartial accountability, for example, by investigating ways to encourage greater engagement of civil society to hold states and companies accountable.
- We fully agree with the IGF that the lack of universal implementation of a norm is problematic, and wholeheartedly support the need to further investigate the reasons for the "digital security divide" and how it creates barriers preventing the implementation of norms. While we support the need to help less 'prepared' communities adopt international best practices established by more 'experienced' nations that have been dealing with cybersecurity challenges for years, we would specifically encourage further thinking around the challenge of identifying mechanisms that encourage sensible cybersecurity behavior at individual level as well.

In this document, we also provide answers to the questions asked by the BPF, which we hope will positively contribute to its broader work. The Cybersecurity Tech Accord signatories also look forward to continuing to engage with the IGF in person at the next annual meeting taking place in Paris in November 2018.

How do you define a culture of cybersecurity?

The importance of developing and maintaining a culture of cybersecurity cannot be overstated as nations of all size and economic development pursue the benefits of digital transformation technologies. To that end, we agree with and applaud the inclusion of the section dedicated to building a culture of cybersecurity in the background paper to the IGF Best Practices Forum on Cybersecurity, *Cybersecurity Culture, Norms and Values,* and echo its main tenets.

Developing a resilient culture is inherently a multi-stakeholder process, with roles for government, industry and civil society in supporting its establishment in countries across the development spectrum.

Several of our signatories have long played a role in socializing and promoting cybersecurity awareness in the public and private sectors and have worked to support the development of informed and effective cybersecurity policies in emerging economies through various forms of engagement.

Examples of our signatories' contributions include:

- CISCO: Network Security Policy: Best Practices White Paper.
- Microsoft: security baselines for critical infrastructure protection ; national cybersecurity policy frameworks.
- Predica: 5 Essential Practices For Your IT Security To Stay Away From The Bad Guys.
- Arm: IoT Security Manifesto.

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

The Tech Accord is the first-ever global coalition of industry partners, of its size, to come together over foundational cybersecurity principles and commitments, and has grown from 34 to 44 signatories since its launch in April 2018. We see this number growing, and as such we believe that the principles put forward by the group could be counted as an emerging norm for our sector.

The four core principles that all our signatories pledge to uphold through shared commitment and collective action are:

1. We will protect all of our customers and users everywhere.
2. We will oppose cyberattacks on innocent citizens and enterprises.
3. We will help empower users, customers and developers to strengthen cybersecurity protection.
4. We will partner with each other and with likeminded groups to enhance cybersecurity.

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.

The Cybersecurity Tech Accord signatories believe that the background paper sufficiently captures the norms put forward and being developed for our sector.

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?

The Framework for Improving Critical Infrastructure Cybersecurity, developed by the U.S. National Institute of Standards and Technology ("NIST Framework"), is a good example of what effectively is quickly becoming an important best practice norm. The Framework has proven to be effective and has therefore quickly gained broad adoption across the world.

While originally developed in the US the Framework is also being adopted in other regions of the world. For example, the Italian government adopted in 2015 their own cybersecurity framework, which focuses on small and medium sized enterprises, largely borrowing from the NIST Framework. Similarly, the Australian Securities and Investments Commission (ASIC) in 2015 issued Report 429 Cyber resilience: Health check (REP 429), which encouraged businesses to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks or to stocktake their cyber risk management practices. Moreover, the International Standards Organization (ISO) has recently approved work on a technical report on "Cybersecurity and ISO and IEC Standards", which seeks to take the NIST Cybersecurity Framework and adapt it to the international environment.

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)?

it is clear that the international cybersecurity norms that have been proposed and agreed to so far, have not been adhered to by nation states, at least not consistently. While there have been examples that have been

promoted as successes, for instance the supposed reduction of cyber espionage in the aftermath of the China-US cybersecurity agreement, successes like that have been few and far between.

While it could be argued that the norms building effort for cybersecurity has failed, it is more likely that we find ourselves in the acceptance building phase, where normative standards become established. While a lengthy acceptance building phase might be common in traditional environments, it represents a significant challenge in the fast-moving online environment. The lack of action is likely to discourage norms entrepreneurs from putting forward new rules of the road, as well as allow for further escalation of tensions in cyberspace.

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

All norms, irrespective of the focus area they have emerged in, have one thing in common. Their acceptance took time, unless they have emerged in a response to a catastrophic event. This is particularly true as it relates to weapons frameworks, an area where cybersecurity is often compared with. Norms adoption and implementation often requires nation-state actors to give up a strategic advantage for the common good, which is a difficult hill to climb under any circumstances.

In the absence of a catastrophic event, the role of civil society has always been colossal. Norms implementation requires a watchdog, formal or informal, that can call out both positive actions by nation-states, and highlight bad behavior. Today this happens too rarely, and when it does, the actions called out are rarely linked with established norms, such as the ones adopted by the UNGGE and referred to in your background paper.

Moreover, while attribution in cyberspace is difficult, it is not impossible, and it is important that investments in this space continue. Moreover, much can be done by encouraging governments to make their cyberwarfare doctrines public, encouraging transparency and investment in implementation of risk-management policies.

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 user at an individual level and nations at a macro level results in different challenges for them, based on their different online experiences. Users connecting for the first time in 2018 are entering a cyberspace beset by sophisticated cybersecurity challenges and threat actors. They have a steep learning curve ahead of them before they will be able to truly act as responsible and protected users of the global internet.

At the same time, coming online today also means that users have more resources at their disposal to support a digital transformation, providing them with opportunities to leapfrog the challenges of previous generations. Similarly, the threats they encounter might diverge as different modes of connectivity, for example mobile, create new ways of operating online and new business models, not always accounted for by "traditional" providers. Finally, the cultural context in which the users come online may also be different.

Therefore, while countries coming online today should seek to adopt established international best practices, such as the Budapest Convention on Cybercrime or aforementioned NIST Cybersecurity Framework, they should not forget the need to adapt these best practices to their own context. Learning from practices that work well is critical, as it often allows for a relatively quick adoption of models that work, driving security practices sooner, and creating room for adaptation later on. Conversely, delivering security frameworks from scratch is often time intensive and leaves users exposed – a trap many organizations, and countries have fallen into.

About the Cybersecurity Tech Accord

The Cybersecurity Tech Accord is a public commitment among 44 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace. Learn more at www.cybertechaccord.org