TECH ACCORD

IGF Best Practice Forum on Cybersecurity

Cybersecurity Tech Accord response to request for comments

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'. We have followed and supported the work of the BPF since the Cybersecurity Tech Accord was created and are committed to furthering its objectives. We believe that diverse perspectives – from governments to civil society and the private sector – must be included in the dialogue on internet governance, so that we can together work towards decisions that reflect and impact a wide range of perspectives and interests. These types of multi-stakeholder coalitions are, in the end, essential to the survival of the cyberspace that we all share and are delighted to see the IGF complementing other important initiatives in this area.

In particular, the signatories to the Cybersecurity Tech Accord are supportive of the work the BPF has taken on over the past two years, which seeks to provide a comprehensive view of the ongoing work on cybersecurity in the context of international peace and stability. With that in mind we welcome both last year's work on norms development and this year's attempt to identify best practices related to implementation of the different elements contained within various international agreements and initiatives on cybersecurity.

While we provide detailed responses to the questions posed later in the document, we wanted to first clarify some of the assessments made about the Cybersecurity Tech Accord. While we believe the attempt to compare the different initiatives identified is worthwhile, we recommend that the BPF doesn't look at the developments in this space only through the prism of government agreement and action. The industry and technical experts have a critical role to play in securing our online environment, sometimes as individual entities, sometimes in partnerships within the industry, and more often than not together with governments and civil society. Our principles should be seen in that context.

For example, the principle that commits us to oppose cyberattacks on innocent civilians, is not, as your document highlights, less relevant to state norms, but in fact critical to it. We have in recent years seen numerous attempts by governments to try and tamper with products and services. A joint industry commitment to prioritize security and privacy of our products and services directly influences how government proposals such as those are devised, and if they are implemented.

Furthermore, while a number of the issues that you compared in the document are not highlighted in the principled commitment that brought the Cybersecurity Tech Accord signatories together, it is important to note that the group has done substantial work to implement the issues raised. We highlight these throughout our response, but whether it is work on definitions, commitment to multistakeholder approaches, dedication to vulnerability disclosure policies and capacity building, as well as recommendations issued on vulnerability equities processes and confidence building measures – the Cybersecurity Tech Accord signatories have tackled all of these and more in its first year and a half of existence. More than that, we have supported and actively engaged in a number of initiatives that you have highlighted, whether expressing a voluntary commitment to their implementation, or responding to government directive, such as with the EU Network and Information Security Directive.

The Cybersecurity Tech Accord and its signatories remain available to provide further details on our work, as well as remain available for detailed comments on this submission. For more information, please contact the secretariat at info@cybertechaccord.org.

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!***

   The Cybersecurity Tech Accord is one of the initiatives mentioned in the document. While our initiative is correctly highlighted as work within a particular stakeholder group (i.e. industry), it is important to highlight that the group has endorsed and supported various other initiatives that were identified as part of your research. These include the Paris Call for Trust and Security, work on MANRS, as well as the efforts of the Global Commission on Stability in Cyberspace.

In addition, we recommend that he BPF investigates the work of the UN High Level Panel on Digital Cooperation that the Cybersecurity Tech Accord also contributed to, as well as the efforts of the World Wide Web Foundation on the contract for the web. When it comes to capacity building, we also recommend that the BPF reaches out to the ongoing work by the Global Forum on Cybersecurity Expertise and other similar initiatives.

Finally, it is important to note that the Cybersecurity Tech Accord signatories have strived to work not just amongst themselves, but reach out to other stakeholder groups, and are for example hosting an event at IGF to deepen cooperation with civil society.

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?***

   Examples of how the Cybersecurity Tech Accord signatories implement its commitments to the four principles are included throughout this document. In addition to the efforts we engage in as a group, individual signatories also live the principles every day. We recommend that the BPF takes a look at the report[1] we published on the group's first year anniversary, highlighting the milestones reached.

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?***

   The Cybersecurity Tech Accord signatories welcome the analysis the BPF has engaged in to identify elements of the debate that are frequently repeated across different fora and initiatives. Nevertheless, we believe that the elements identified vary significantly in terms of the role they play in cybersecurity norms conversations and should not be conflated within a single category. With that in mind, we recommend that the BPF creates a framework to guide its analysis that focuses on:

   - **Foundational principles**: The foundational principles identified within this category should guide any development and implementation of cybersecurity norms, and/or binding agreements. We believe that the commitment to multistakholderism and international law, including the UN Charter and human rights elements retained within it, which BPF identified, are critical to the success of any effort in this space. Other principles, such as commitment to accountability or cooperation might also be considered in this context.
   - **Implementation efforts:** Two elements identified by the BPF, capacity building and confidence building measures (CBMs), are not as much part of the agreements, but efforts to drive their implementation. For example, investments in capacity building in cyberdiplomacy are critical for governments around the world to be able to participate in cybersecurity norms discussions. Similarly, it is important to increase efforts to build capacity within the technical community and civil society to work in this space. Building on that, CBMs go a step further and look to implement specific agreements to discrete proposals that serve to increase cooperation and reduce tension in cyberspace. The Cybersecurity Tech Accord signatories have recognized the critical role CBMs play and issued a set of recommendations in this space earlier this year[2].
   - **Initiatives with broad support**: The final category we propose BPF uses are initiatives with broad support that aim to drive positive change towards security and stability in cyberspace. The Cybersecurity Tech Accord signatories particularly welcome the fact that work on vulnerability

[1] Cybersecurity Tech Accord, Annual report 2019: https://cybertechaccord.org/uploads/prod/2019/03/2018report.pdf

2Reducing tensions in cyberspace by promoting cooperation, 2019: https://cybertechaccord.org/reducing-tensions-in-cyberspace-by-promoting-cooperation-cybersecurity-tech-accord-publishes-a-set-of-recommendations-on-confidence-building-measures-in-cyberspace/

disclosure and vulnerability equities policies has been identified, as these are initiatives that we have taken on as part of our group[3].

- **Definitions:** There have been numerous attempts to reach a common understanding of core terms in cybersecurity, such as cyber threats or cyber attacks – the two terms identified by the BFP. These included work within the initiatives highlighted[4], but also in national legislation, and in various standardization initiatives. The Cybersecurity Tech Accord signatories believe that while work on common definitions is clearly needed, this is not something that the BPF engages with, but encourages other efforts, in particularly those focused on CBMs to take on.

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?*

Perhaps not surprisingly, the Cybersecurity Tech Accord signatories believe there is a clear value in agreements such as these, as they establish and promote good cybersecurity practices. We firmly believe that the Cybersecurity Tech Accord has driven a change in industry behavior when it comes to cybersecurity. We are equally convinced that the commitments made have played an important role in signaling to the online community at large what acceptable and what unacceptable behavior in this space is and should be – whether by industry or governments. With that in mind, we have also endorsed initiatives such as the Paris Call for Trust and Security, which we believe also helps build agreement around the core norms and principles our community should endorse if we wish to preserve the open, free, and secure internet we know today.

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

It is our experience that when there is will, there is a way. We have therefore been delighted to see the Cybersecurity Tech Accord grow from 32 signatories at its inception to over 100 today. The rapid growth demonstrates that there is a commitment in the industry to establish best practices, implement clear principles, and drive normative discussions.

Having said that, we have found that even within one stakeholder group, there needs to be a level of flexibility that allows for different business models and approaches to thrive. For example, while the Cybersecurity Tech Accord signatories have agreed to putting vulnerability disclosure policies in place, the group has opted not to impose a particular form these should take, but left it to the individual companies to select the approach that works best for their business model and needs.

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?*

Today's technology environment develops with breakneck speed and none of the solutions we have can simply be defined as black or white, but can be used for both beneficial and nefarious purposes. As a result, developing regulations and setting standards in this space can be challenging. This is particularly the case if the agreements do not focus on outcomes, but attempt to prescribe a particular course of action – one that might be out of date in less than six months' time. Many, if not all, the documents highlighted by the BPF therefore have the potential to have adverse effects.

[3] Recommendations on vulnerability equities processes, 2018: https://cybertechaccord.org/government-vulnerability-handling/

Commitment to vulnerability disclosure, 2019: https://cybertechaccord.org/the-importance-of-vulnerability-disclosure-policies/

[4] Cybersecurity Tech Accord put forward a set of proposed definitions in 2018: https://cybertechaccord.org/for-comment-cybersecurity-definitions/

While this is not the place to comment on any particular agreement, an example worth highlighting are the prolonged discussions on the Wassenaar Agreement's List of Dual-Use Goods and Technologies and the Munitions List. In 2013, France and UK proposed to amend the list to cover intrusion software and IP network communications surveillance systems. The proposal had good intentions and it stemmed from the concerns of non-government organizations that certain repressive governments were able to use such software and systems to eavesdrop on dissidents and reporters within their societies. However, the way the issue was handled initially posed a threat to vulnerability research, resulting in negative consequences for cybersecurity.

We highlight this example that even the best laid proposals do not always achieve the intended result. That does not however mean that we should give up and stop trying. More than anything, this example shows the need for multistakeholder consultations to determine how a particular norm, principle, or requirement could be implemented effectively. We strongly believe that together we can work towards a safer, more secure, and above all, trusted online environment.

.

About the Cybersecurity Tech Accord

The Cybersecurity Tech Accord is a public commitment among over 100 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace. Learn more at www.cybertechaccord.org