The Cybersecurity Tech Accord response to GCSC's request for comments on the Norm Package Singapore

The Cybersecurity Tech Accord signatories welcome the work of the Global Commission on the Stability of Cyberspace on promoting awareness and understanding of issues related to international cybersecurity, peace and stability, and in this context the Singapore norms package. We share the Commission's concern that an increasing number of nations see cyberspace as an unconstrained area of conflict. Indeed, in recent years, malicious actors with motives that range from criminal to geopolitical have inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free, and secure internet. We have seen attacks on the availability, confidentiality, and integrity of data, products, services, and networks that have demonstrated the need for constant vigilance, collective action, and a renewed commitment to cybersecurity.

As highlighted by the Commission, both public and private entities need to act responsibly when managing their shared interest in cyberspace. In fact, that is the motivation that has driven us to agree to the Cybersecurity Tech Accord in 2018. Today, the Cybersecurity Tech Accord is an expanding industry group of 79 global companies, committed to protecting and empowering individuals online and to improving the security, stability and resilience of cyberspace. Our signatories are aligned with the Commission's objective of addressing urgent cybersecurity needs by identifying and promoting operational norms that can help make cyberspace more secure. In an increasingly interconnected world where technologies are exploited to carry out malicious actions, establishing norms for cybersecurity and achieving global acceptance of these norms is a fundamental step to bring predictability, stability, and security to the international environment.

We particularly support the first three norms the Commission proposes. While we highlight certain potential changes, the Cybersecurity Tech Accord signatories can already see how these will help clarify debate in this space. However, in our opinion, more work is needed on the other four, by either clarifying their scope or by reflecting on why we need a norm for practices that are already considered banned in national laws around the world.

The Cybersecurity Tech Accord signatories also welcome the Commission's openness to feedback and encourage the group to consult even more widely and earlier in the process in future. With that in mind, we would welcome further clarity on the process that the Commission will follow in establishing its recommendations on the way to achieve cyber stability in the international peace and cybersecurity architecture. Furthermore, we welcome the opportunity to provide additional feedback on how current norms are supported and how to put them into operation, in particular keeping in mind the nature and commitment of the Cybersecurity Tech Accord as a group.

In conclusion, we believe that the Commission is unique in its ability to bring together groups from across different sectors and geographies in this space and are pleased that its efforts have already resulted in a meaningful evolution of dialogue on international norms related to the security of cyberspace. We also strongly support the Commission's objective of building on these norms by encouraging further discussions and by working on a definition of cyber stability and on a set of recommendations on what the wider international peace and security architecture needs to do to meet that definition. We believe that focusing on adoption and implementation of the Commission's proposals would be a much more meaningful contribution than working on further norms.

Norm to Avoid Tampering: "*State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace*."

Norm: The Cybersecurity Tech Accord signatories have provided feedback on this norm earlier and we appreciate seeing that many of our recommendations have been integrated. We strongly support this norm and agree that state and non-state actors have a responsibility to protect the internet ecosystem. The group, as well as individual signatories have on several occasions encouraged the international community to take this approach seriously by establishing norms that compel state and non-state actors not to introduce or exploit vulnerabilities in software or hardware products.

With regard to the wording of the norm, we believe that it would particularly benefit from a clarification that would signal to state and non-state actors that any introduction of vulnerabilities into the system or negligence in dealing with similar practices by other actors would be sanctioned. In addition, it is unclear to us how it would be determined whether a particular online event would substantially impact the stability of cyberspace and would propose that that limitation is omitted. We therefore propose the following change: "*State and non-state actors should not tamper, with products and services in development and production, nor allow them, purposely or negligently, to be tampered with, if doing so may ~~substantially~~ impair the stability of cyberspace*."

Background notes: In the notes, the expression "*targeted state action*" is not explained in any substantial detail and no definition is provided (page 9). Indeed, a single example is given of what it could entail (targeted interception and tampering of a limited number of end-user devices in order to facilitate military espionage or criminal investigations). It is critical that that is further defined.

Moreover, it is important to remember that the attacking party might not always understand the role of the particular entity they are targeting in the larger information and operational technology environment. Some vulnerabilities might be, in fact, interpreted as benign on their own and, as such, not capable of compromising the non-governmental use of the Internet. In reality, all vulnerabilities are risky for the Internet ecosystem because, no matter how irrelevant they might appear, they all have the potential to compromise the security and stability of products and services in their entirety. We therefore encourage the Commission to omit this limitation and encourage all governments to refrain from introducing vulnerabilities into IT products or services.

Implementation: Two of the core commitments of the Cybersecurity Tech Accord directly relate to this norm: the commitment that we will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities; as well as the pledge that we will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.

We would like for these industry principles to be adopted more broadly, but we acknowledge that given the diversity of the online ecosystem the implementation of that commitment might have to be done through a variety of approaches and standards. Moreover, it is important to underline that the implementation can only be done with responsible behavior on behalf of states, which would have to commit to not legally compel companies to tamper with their products and services.

Supporting documents: Cybersecurity Tech Accord commitment.

Examples of breach: While not necessarily what the writers of the norms envisioned, it is possible to imagine that the use of the Australian Assistance and Access Bill 2018 could constitute a breach. The legislation not only compels companies to hand over user data they have easy access to, but also to build the ability for themselves to intercept this data when they don't and therefore has the potential to introduce systematic weaknesses that could harm the data security of users. We encourage the Commission to consider such legislative moves as it assesses the norm further.

Norm Against Commandeering of ICT Devices into Botnets: "*State and non-state actors should not commandeer others' ICT resources for use as botnets or for similar purposes.*"

Norm: Botnets and other automated threats pose a direct and growing challenge to nearly all aspects of IT use, from personal computing by private individuals to cloud-enabled enterprise management on a global scale by multi-national corporations. Therefore, we strongly agree with this norm and with the need for state and non-state actors to commit to refraining from the practice of commandeering ICT devices for use within a botnet. Having said that, it is important to clarify that such activity conducted by non-state actors is already illegal in many jurisdictions and that there is therefore no need to include this in a norm, given the existence of a strong legal practice.

Background notes: While the norm itself is relatively solid, the background introduces a level of confusion into how the norm is intended to be interpreted. For example, it is not clear why the background notes focus exclusively on devices, and in particular on consumer devices, whereas the language of the norm – in our opinion rightly – talks about ICT resources in general. It is not clear why a device used by a consumer would be offered different protections from a device deployed in an enterprise. Moreover, if the norm is supposed to be complementary to the norm related to tampering with product and services prior to their release, the scope of work should be similarly defined as broadly and incorporate all ICT resources.

Similarly, while the text of the background notes talks about not commandeering devices *en masse*, this is not clear from the norm, which does not specify the level of activity that is prohibited, again in our opinion rightly so.

Implementation: In addition to government commitment to refrain from commandeering ICT resources, much can be done to stop the threats that botnets pose. Examples include (1) working with industry to develop flexible security standards for the IoT market; (2) promoting market incentives for adoption of these flexible security standards; (3) facilitating coordinated public-private action against botnets and related threats; and (4) engaging with international partners to facilitate global action against botnets and related threats.

Supporting documents: The Paris Call for Trust and Security in Cyberspace (Paris Call) issued by the French government in November 2018, which we endorsed as a group, stresses the need to "*prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure*".

Examples: The 2014 Sony PlayStation and Microsoft Xbox attacks that are thought to have originated from North Korea can be seen as examples of breach of this norm. The Mirai attack on Dyn in 2016 can be considered an example as well.

Norm for States to Create a Vulnerability Equities Process: "*States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favour of disclosure.*"

Norm: We strongly support this norm and have argued for adoption of such policies in the past. In September 2018, we published a statement regarding the need for governments to do more and say more on vulnerability handling. In December 2018, we followed up with a blog post regarding the UK government's publication of its vulnerability equity process.

Nevertheless, we still have a recommendation to make and propose that the Commission omits the term *flaw* in the norm. It is not clear what is meant by the term or what it adds that is not adequately covered by the term vulnerability in this context.

Background notes: While we support the norm, the background notes make an important clarification that if a government decides to disclose a vulnerability it should do so in a responsible manner. That is a critical clarification and it is important to ensure that that is understood. In a similar vein it would be important to include that, if a government decides to retain vulnerabilities, it needs to ensure that these are stored in a secure location and protected.

Implementation: International organizations and industry groups can certainly play a role in encouraging governments to take a step forward on vulnerability disclosure. The Cybersecurity Tech Accord has done so in the above-mentioned statements and our signatories have been active in partnering with like-minded organizations to push this forward. This and other initiatives can help fuel a change of mindset with governments moving from investing in offensive to investing in defensive technologies. Moreover, the adoption of a vulnerability equity process would be an important step forward in relation to the establishment of confidence building measures, which are critical to trust between states.

Supporting documents: Please see the above-mentioned statements by the Cybersecurity Tech Accord.

Examples: Very few countries have vulnerabilities equities processes in place, and an even smaller number has been transparent about what the process is and who the entities involved in the decision making are. At this stage, outside that small number, most countries could be considered in breach of this norm.

Norm to Reduce and Mitigate Significant Vulnerabilities: "*Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity*."

Norm: We agree that one of the most effective approaches to minimizing the possibility and potential impact of cyber-attacks is to leverage rigorous processes, tooling, and training to securely develop, operate, and maintain ICT products and services. Unfortunately, no system is entirely free of security issues and this is why it is fundamental that external parties report vulnerabilities to manufacturers and vendors so that they can take appropriate steps to resolve them. Moreover, it is important to underline that, despite companies' efforts to protect customers, cyber threats are not an issue that can be solved by each company acting alone. Efforts by businesses, developers and security researchers need to be complemented by a broader international framework where all actors involved, including governments, are compelled to do their part in protecting cyberspace. This is particularly urgent considering that essential services are often the most vulnerable to cyber-attacks, not only for the high probability of being a target but also because they are often not adequately protected. Efforts in this area will be fundamental to ensure that malicious activities online do not impact on the security of our increasingly interconnected societies.

Background notes: The notes generally refer to the need to "*share information that would assist in fixing security vulnerabilities or help prevent, limit or mitigate an attack*" (page 15). It is worth adding that the process of disclosing such vulnerabilities is all but straightforward and that it is important that vulnerabilities are shared in a controlled way, according to a mechanism defined as Coordinated Vulnerability Disclosure (CVD). This mechanism requires the companies affected and the reporter of a vulnerability to work together to minimize any risks for system owners, third parties, and the society.

Implementation: For this norm to result in consistent implementation, it is important to not only have a clear procedure to follow when reporting vulnerabilities but also to establish a culture of transparency and trust. Reporters should be aware that they will not be unduly penalized and that their efforts will not result in any legal action. Dialogue within the industry can help in this regard but most importantly companies should make their CVD policies available on their website so that reporters can be aware of the steps to take when reporting a vulnerability.

Supporting documents: In September 2018, the Cybersecurity Tech Accord published a statement endorsing the Global Forum on Cyber Expertise (GFCE)'s Global Good Practices on Coordinated Vulnerability Disclosure (CVD), which, in our view, represents the most comprehensive guide on this topic.

Examples: Entities that do not adopt and communicate their coordinated vulnerability disclosure policies could be considered in breach of this norm.

Norm on Basic Cyber Hygiene as Foundational Defense: "*States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene*."

Norm: Cyber hygiene is about thinking proactively about our cybersecurity and that is not easily solved with laws and regulations alone. Rather than looking at potential regulatory frameworks, we would therefore encourage states to reflect on and implement strategies and measures to spread awareness around the importance of cyber hygiene among users and citizens.

Background notes: The Cybersecurity Tech Accord signatories are somewhat concerned by the tone used in the background notes. For example, the end of the first paragraph implies that every internet user is working with an inherently unsafe and dangerous tool. It completely omits any good cybersecurity work and places no responsibility on attackers online or on the role of governments to set baseline standards of behavior in online conduct to prohibit or otherwise propose and enforce appropriate penalties for attackers.

The background notes also do not differentiate between the different stakeholders online and their need for differing levels of protection. The long-established principle of risk-management – based on the need to understand and protect the most critical assets – is replaced by a broad statement on the need to regulate basic cyber hygiene. The note gives a positive outlook on automated information sharing with users, without considering that such a system would more broadly spread the knowledge of potential vulnerabilities.

Implementation: Nowadays, technology pervades every aspect of our life and people become familiar with the internet from a very young age. Implementing this norm would therefore require education on cyber hygiene to start in schools and to continue throughout people's different educational and career paths, adjusting to the specificities of the users' interactions with technologies. In general, establishing a common baseline of cyber hygiene practices would already be an improvement vis-à-vis users' current lack of cybersecurity literacy. There are other ways governments can invest in public awareness; successful efforts have included national awareness events (such as dedicating a national cybersecurity awareness week or month), public service advertising campaigns, dedicated websites and online guidance, social media campaigns, and school events. Another important way the government can promote cybersecurity awareness is by making available aggregate and publicly disclosed data about cybersecurity incidents to enable researchers, policymakers, and average citizens better understand the scope and contours of cybersecurity challenges.

Supporting documents: It could be useful to look at BSA's "International Cybersecurity Policy Framework".

Examples: While numerous states have adopted basic cybersecurity policies, they have not been implemented at the broad level this norm envisions. An example of a breach would therefore be any country without basic cyber hygiene policies and implementation in place.

Norm Against Offensive Cyber Operations by Non-State Actors: "*Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur*."

Norm: The Cybersecurity Tech Accord signatories believe that this is a matter for national cybercrime legislation and has no place in an international norm.

Background notes: The tech sector remains the first line of defense when it comes to cyber-attacks. While technology companies have a big role to play in protecting against malicious activities, in part because they have an abundance of in-house expertise and have to protect their own networks and respond to cyber-attacks, it would be a mistake to think that the private sector by itself can prevent or stop the risk of cyber-attacks any more than it can prevent any other types of military attacks.

To our knowledge, no government has sanctioned hack back for the private sector, and it is unclear which private sector entities advocate for it. However, states have explicitly granted non-state actors the authorization to conduct offensive operations. This is an activity that should be covered by other norms proposed in the Singapore package.

In line with that, the proposed norm would benefit from much more clarity as to what type of issue we are trying to address. Hack back, active defence, and offensive cyber operations all have different meanings, and are also different from intrusive actions that cybersecurity defenders sometimes conduct on behalf of their clients, such as pen testing. Without further definitional work, this norm does not bring additional clarity to the issue.

Implementation: A beneficial implementation of the concepts covered by this norm would be harmonized national approaches and willingness by states to prosecute perpetrators.

Supporting documents: The Paris Call (see above) stresses the need to "*take steps to prevent non-State actors, including the private sector, from hacking back, for their own purposes or those of other non-State actors*".

Examples: Given the lack of clear definitions in this space more broadly, including in this norm, where active cyber defense, offensive operations, and hack back seem to be used interchangeably, it is difficult to provide concrete examples of when this norm was breached. For instance, many of the frequently quoted examples are not destructive offensive attacks, but mere monitoring of activity.