GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

CALL FOR CONTRIBUTIONS ON THE 2019 BPF ON CYBERSECURITY:

SUBMISSION OF THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Global Commission on the Stability of Cyberspace (GCSC) appreciates the opportunity to contribute to the 2019 IGF Best Practice Forum on Cybersecurity and give its input on the review of cybersecurity agreements. Having been a regular contributor to previous iterations of the Internet Governance Forum and BPF on Cybersecurity,[1] the GCSC commends the valuable work the that Best Practice Forum is undertaking and hopes that its feedback will provide useful guidance in assessing relevant processes in the field of cybersecurity.

Question 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?

The Paris Call for Trust and Security in Cyberspace refers to five of the GCSC norms, making explicit reference to the Commission's flagship norm on protecting the public core of the Internet. Other norms referred to in the Call include preventing malign interference with electoral infrastructure, establishing a vulnerabilities equities process, ensuring basic cyber hygiene and prohibiting offensive cyber operations. The Paris Call for Trust and Security in Cyberspace is a high-level declaration in favor of the development of common principles for securing cyberspace. It was launched in November 2018 at the Internet Governance Forum by President Emmanuel Macron of France. It has already gained the backing of 552 official supporters, in which the GCSC is proud to be included.

The Commission also aims to participate in and engage with other initiatives and processes. Several GCSC members were involved the United Nations Secretary-General's High-Level Panel on Digital Cooperation, which submitted its report The Age of Digital Interdependence to the UN Secretary-General on 10 June

[1] In recent years the Global Commission on the Stability of Cyberspace has been a regular participant and session organizer of the United Nations Internet Governance Forum. Participation and submissions include:

- Internet Governance Forum 2017 Geneva, zero-day event
- Internet Governance Forum 2017 Geneva, submission to and Participation in the Best Practice Forum on Cybersecurity
- Internet Governance Forum 2018 Paris, panel session
- Internet Governance Forum 2018 Paris, submission to and Participation in Best Practice Forum on Cybersecurity

2019. Furthermore the Commission has openly engaged with the United Nations Open-Ended Working Group[2] and the Group of Governmental Experts,[3] hoping to inform those processes whilst ensuring the participation of non-state stakeholders in the traditionally state-led dialogue of the UN First Committee.

As mentioned above, the GCSC norms have been acknowledged, welcomed and adopted by a number of organizations and initiatives. Whilst awareness and adoption is encouraging, effective implementation of these norms – as well as norms and CBMs developed elsewhere, such as those agreed upon in the United Nations Group of Governmental Experts Report of 2013 & 2015 – will prove to be the crucial step in achieving stability in cyberspace.

Question 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?

The public core norm was codified in the EU Cybersecurity Act, recently approved by the EU Parliament and Council and extending the mandate of the European Union Agency for Cybersecurity (ENISA). Similarly, the report of the UN Secretary-General on the Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels highlights the work of the Commission on norms of responsible behavior for reducing the risks to cyber stability.

Norm-creation cannot however be the sole focus of international cooperative agreements, and further steps should therefore be taken in order that stakeholders actually implement these 'rules of the road', ensuring that stability has a lasting effect and reducing the risk of conflict and uncertainty in cyberspace. Having proposed eight critical norms, which are supported by underlying fundamental principles, the GCSC has since focused on defining what stability entails and which actors have a role to play in achieving this equilibrium.

The Commission has sought to foster discussion on common understandings of responsible behavior and engage with stakeholder groups at forums and conferences across the globe. Going beyond this, the Commission intends to extend the debate by mapping out the international security architecture of actors in cyberspace and developing a framework for the implementation of its proposals. The objective of this would in part be to identify potential institutional homes for the Commission's proposals and recommendations.

[2] United Nations General Assembly, Resolution adopted by the General Assembly on 5 December 2018, A/RES/73/27 (2019) https://undocs.org/en/A/RES/73/27

[3] United Nations General Assembly, Resolution adopted by the General Assembly on 22 December 2018, A/RES/73/266 (2019) https://undocs.org/en/A/RES/73/266

In formulating its final report, the GCSC's work has been informed by valuable input and feedback,[4] though more widespread success will be dependent on the involvement of other stakeholders in a more active role. Implementing norms involves taking concrete steps to give them force, thereby making them operational. The current mode of engagement is not sufficient to reach the notion of stability as developed by the Commission and understood by the cyberspace community at large, as all too frequently non-state actors are excluded from discussions that occur in the state fora (such as the United Nations First Committee). In addition, proposals are sometimes developed by one stakeholder group but are addressed to or affect another. These therefore become unilateral rather than cooperative measures, as there is no awareness or understanding of when and how to act upon them. As a next step in its framework and as part of its recommendations, the Commission will suggest the creation of Communities of Interest (COI), encouraging stakeholders to come together and drive forward the change needed to ensure that norms and stability measures are implemented, adhered to and enforced.

The formation of a Community of Interest is by its very nature ad hoc and bottom-up: the exact composition and mission of such a COI is always derived from the group itself. However, some shared principles for a COI are usually identifiable: it should derive from an existing corpus or agreement of norms, it should have a singular focus on one aspect (for instance on one norm), it should be created at least with the tacit agreement of the host processes primary sponsors and accept the same basic principles (for instance the applicability of international law). Moving forward it may even be possible to identify a best-practice template of how COIs should be stood up and implemented. This would ideally allow various norm-setting processes as diverse as the UNGGE, the Paris Peace Forum, the Tech Accord and others to mutually share a similar COI model for example. This in itself would be an important factor to reconciling various process to each other, and finding common definitions in implementation, adherence and potentially even enforcement.

Similar groups at the multilateral level are currently referred to as "like-minded nations". Given the complexity and multistakeholder nature of the cyberspace ecosystem, an innovative approach is necessary whereby states and non-state actors can work together to fulfill their respective roles in a collaborative and complimentary way. State-focused norm processes will increasingly require non-state actors to be effective in norm implementation, adherence and even often enforcement. For this reason, the term "Community of Interest" is more applicable than the term "like-minded actors", given the different roles of the state and non-state actors and their various levels of engagement. In general, the Internet has a long tradition in "communities of interest" driving forth change. A principle element of the technical standard process of the Internet Engineering Task Force is the BOF (Birds of a Feather) Group, a special interest group of like-minded actors that can meet for virtually any reason, while dedicated working groups often drive implementation of an agreed standard before others do. This could be a potential model to follow and build upon.

In order to make greater progress on norm and stability measure adoption, implementation, accountability and, to some extent, enforcement, a novel approach would be to designate "communities of interest"

[4] See the Request for Consultation on the Singapore Norm Package https://cyberstability.org/research/request-for-consultation-norm-package-singapore/, as well as the subsequent Request for Consultation on the Definition of the Stability of Cyberspace https://cyberstability.org/news/request-for-consultation-definition-of-stability-of-cyberspace/

around particular proposed norms or particular stability recommendations. For example, the CSIRT community could form a COI around implementing and monitoring the UN GGE norm aimed at protecting CSIRTS and work closely with governments and international institutions on this issue. The Internet Governance technical community could help advance, implement and monitor the Commission's proposed norm on protecting the public core of the Internet. The capacity building community can help advance norm adoption and implementation especially in less developed countries. Interested parts of the private sector, academia and civil society could work to construct an accountability mechanism and process. In these cases, and many others, appropriate Communities of Interest should be identified and organized to make more concerted progress than the current more piecemeal approach has produced.

Continuing in its mandate of developing proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace, the GCSC will therefore be proposing that an issue-focused approach is developed for identifying special interest groups that might take on the implementation of norms and policies developed by the international cyberspace community at large. This will be further defined in its final report, which is due at the end of 2019 and which includes a number of recommendations targeted at specific actors.

Question 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?

a. **Furthers multi-stakeholderism:** identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.

The GCSC is founded on a multistakeholder approach and considers this to be one of the most important building blocks of any cybersecurity-related agreement. Without the effective involvement of all stakeholders in the development of policy and decision-making there can be no basis for achieving lasting stability. Whilst states are traditionally the dominant actor in international peace and security, they only make up one of three stakeholder groups in the cyberspace ecosystem. The private sector owns much of the physical infrastructure on which cyberspace depends, and the technical sector is responsible for the development of protocols and standards that ensure it continues to operate efficiently. The development of sustainable, inclusive and principle-based solutions in cyberspace therefore require the effective participation of all stakeholder groups. Consequently, a multistakeholder approach is present throughout the GCSC's proposals and is reflective of the nature of the Commission itself.

b. **Reference to International Law:** whether the agreement reflects on the importance of aligning international law.

Tying norms and policies to existing international law is important as it shows a viable path towards adoption and implementation of those provisions. It might also assist in identifying the problem areas, where there are significant threats to cyberspace but as yet no body of law seeking to protect the stakeholders and rights at risk. This may also lead to areas of potential cooperation, informing those approaches that focus on confidence and capacity building.

c. **Vulnerability equities processes:** the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.

The GCSC released a Norm for States to Create a Vulnerability Equities Process in its Singapore Norm Package. This norm focuses on state actors but works in combination with the Norm to Reduce and Mitigate Significant Vulnerabilities, which addresses non-state actors as developers and producers of products and services on which the stability of cyberspace depends. The Norm to Avoid Tampering also calls for state and non-state actors to avoid tampering with products and services in development and production, effectively outlawing the insertion of vulnerabilities during the supply chain.

Recently certain governments have taken steps to publish elements of their vulnerabilities disclosure processes, amongst them the United Kingdom, the Netherlands and the United States. This has in part been to alleviate concerns and foster trust that they are indeed taking steps to mitigate some of the issues involved in the handling and retention of vulnerabilities. Such policies have in fact been in place and been implemented for a longer period of time, but only now is it becoming more clear what approaches are being taken to address issues in vulnerabilities disclosures. The GCSC sees these as positive developments, though more can be done to meet the criteria involved in reducing the effects of exploitation of vulnerabilities.

The existence of such processes can act as a confidence-building measure between states in that it provides some assurance that relevant equities and competing interests are fully considered. In addition, though the actual decisions reached in individual cases may, out of necessity, remain confidential, there should be transparency on the general procedures and framework for reaching such decisions. If a government or any other entity decides to make a disclosure, such disclosure should be made in a responsible manner that promotes public safety and does not lead to exploitation of that vulnerability.

d. **Reference to Capacity Building:** whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.

e. **Specified CBM's:** whether the agreement describes or recommends specific Confidence Building Measures.

Capacity building and confidence building measures (CBMs) together form an important part of norm implementation. These are about creating a foundation that empower stakeholders to take action and implement their norms.

f. **Reference to Human Rights:** whether the agreement reflects on the importance of human rights online.

The recognition of fundamental rights and freedoms is crucial to the object and purpose of cybersecurity agreements. The key is for these agreements to work alongside human rights provisions. This can be most clearly seen in the identification of threats and risks in cyberspace, and through the adoption of norms and policies that seek to protect the rights of individuals and stakeholder groups. Agreements in cyberspace should seek to give human rights provisions their full effect, by developing understanding of the issues inherent in the threats and also by allowing individuals to freely exercise their rights.

Question 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?

Value of many of these agreements reside in the fact that a multistakeholder approach to issues pertaining to international peace and security is required, especially to advance the discussion on norm acceptance and implementation. Civil society and the private sector have a better understanding of what needs to be done in their own communities to ensure broader norm acceptance to reduce the risks these norms seek to address.

Question 5: Have you seen any specific challenges when it comes to implementing the agreement? 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?

One of the challenges of agreeing on norms of behavior in cyberspace is that norms - and the associated practical implementation measures, such as Confidence-Building Measures (CBMs) – are sometimes formulated by one set of actors but expected to be executed by another. This requires that the actor groups, regimes, and initiatives fully recognize each other's mandate or legitimacy. This is not automatically the case.

Working across the cyber regime complex is therefore primarily a question of accepting mutual legitimacy. Any norm, project or initiative that seeks to have a truly global reach and effect on cyberspace must have the support of key actors across the regime complex to succeed. These actors are considered to be legitimate either because of their ability to be representative of their constituents (be it members, citizens, or customers), knowledgeable on the technical details within their field, or the ability to practically effect change. Accepting any one of these definitions of legitimacy is the equivalent to trusting the verdict of these actors to at least be relevant within the wider discourse, and, as the U.S. State department pointed out within their 2014 report, trust among these different state and non-state actors is key to cyber stability.